



# **FOIP Guidelines and Practices**

2009

**Government of Alberta ■**







FREEDOM OF INFORMATION AND  
PROTECTION OF PRIVACY ACT

# **FOIP Guidelines and Practices**

**2009**

**Government of Alberta ■**

*Produced by*

Access and Privacy  
Service Alberta  
3<sup>rd</sup> Floor, Commerce Place  
10155 – 102 Street NW  
Edmonton, Alberta, Canada  
T5J 4L4

FOIP Help Desk Phone: 780-427-5848  
Office Phone: 780-422-2657  
Fax: 780-427-1120  
Website: [foip.alberta.ca](http://foip.alberta.ca)

*Printed copies of this publication are available for purchase  
from Alberta Queen's Printer at [www.qp.alberta.ca](http://www.qp.alberta.ca) or 780-427-4952.*

©Government of Alberta

ISBN 978-0-7785-8563-3

## PREFACE

This publication provides a comprehensive reference tool for the application of Alberta's *Freedom of Information and Protection of Privacy Act* (the *FOIP Act*). It is designed to assist all public bodies that are subject to the Act.

*FOIP Guidelines and Practices* explains the principles of the FOIP legislation and suggests how the Act and Regulation should be understood, taking into consideration the most significant decisions of the Information and Privacy Commissioner. The manual also explains roles and responsibilities with respect to the administration of the Act, and offers guidance on procedural matters.

The manual is intended to offer guidelines and to suggest best practices, not binding rules. Some statements are shown in indented bold text with the FOIP logo beside them. This format is used when the statement is either a policy that Government of Alberta departments and their affiliated agencies, boards and commissions must follow or it is a definitive interpretation of the Act based on Commissioner's Orders. Other statements are shown in indented plain text with the FOIP logo beside them. This format is used when the statement is an important procedural matter that should be considered by all public bodies subject to the Act.

All examples used are provided as illustrations only and should not be used as authority for any decisions made under the Act. This publication is not to be used as a substitute for legal advice. In case of any doubt as to the proper application of the Act, please refer to the FOIP Coordinator of your public body.

The 2009 edition of *FOIP Guidelines and Practices* incorporates amendments to the FOIP legislation up to June 1, 2009, including the *FOIP Amendment Act, 2006* and the new FOIP Regulation (2008). This edition references Commissioner's Orders and Investigation Reports released up to December 31, 2008.

The manual also provides coverage of new subjects, including records relating to audits by the Chief Internal Auditor of Alberta, ministerial briefing books, and disclosure of personal information to a foreign court or tribunal. Also included are new treatments of a number of topics, such as the criteria for excusing fees in the public interest and the exercise of right by guardians. Other changes reflect the government reorganization in March 2008.



# Contents

	<b>Page</b>
1. Purposes and Scope of the <i>FOIP Act</i> .....	1
2. Administration of the <i>FOIP Act</i> .....	23
3. Access to Records .....	47
4. Exceptions to the Right of Access .....	95
5. Third Party Notice .....	211
6. Disclosure in the Public Interest .....	225
7. Protection of Privacy .....	233
8. Records and Information Management .....	305
9. Privacy Compliance .....	319
10. Information and Privacy Commissioner .....	349

## **Appendixes:**

Appendix 1: Definitions .....	369
Appendix 2: Delegation and Assignment of Responsibility Tables .....	383
Appendix 3: Model Letters .....	395
Appendix 4: Model FOIP Request Charts .....	439
Appendix 5: Forms .....	447

## **Indexes:**

<i>Freedom of Information and Protection of Privacy Act</i> and Regulation Citations .....	449
Information and Privacy Commissioner's Order and Investigation Report Citations .....	459
Words and Phrases Defined or Discussed .....	465
Subject .....	473



# Detailed Table of Contents

	<i>Page</i>
<b>1. Purposes and Scope of the <i>FOIP Act</i>.....</b>	<b>1</b>
Overview.....	1
1.1 Purposes of the <i>FOIP Act</i> .....	1
A right of access to records .....	1
Protection of personal privacy .....	1
A right of access to an individual's own personal information .....	1
A right to request correction.....	2
Independent review of decisions .....	2
Scope of the Act .....	2
Public body ( <b>section 1(p)</b> ).....	2
Local public body ( <b>section 1(j)</b> ).....	2
Educational body ( <b>section 1(d)</b> ).....	2
Health care body ( <b>section 1(g)</b> ).....	3
Local government body ( <b>section 1(i)</b> ).....	3
Bodies excluded from the definition of "public body".....	4
1.2 Application of the Act.....	5
Existing procedures for access .....	5
Archival records .....	5
Legal proceedings.....	5
Disposition of records.....	6
1.3 Records Subject to the Act.....	6
Record ( <b>section 1(q)</b> ) .....	6
Personal information ( <b>section 1(n)</b> ) .....	6
1.4 Custody or Control.....	7
1.5 Records Excluded from the Act .....	9
Categories of excluded records .....	9
Certain categories of information in court and judicial records ( <b>section 4(1)(a)</b> ).....	9
Draft judicial or quasi-judicial decisions ( <b>section 4(1)(b)</b> ).....	9
Quality assurance records of health care bodies ( <b>section 4(1)(c)</b> ) .....	10
Records of an officer of the Legislature ( <b>section 4(1)(d)</b> ) .....	10
Records provided to the Ethics Commissioner ( <b>section 4(1)(e)</b> ) .....	11
Records created by or for the Ethics Commissioner ( <b>section 4(1)(f)</b> ).....	11
A question to be used on an examination or test ( <b>section 4(1)(g)</b> ).....	11
Teaching materials ( <b>section 4(1)(h)</b> ).....	11
Research information of employees ( <b>section 4(1)(i)</b> ).....	11
Archival materials ( <b>section 4(1)(j)</b> ).....	12
Published works collected by a library ( <b>section 4(1)(j.1)</b> ) .....	12
Records relating to an ongoing prosecution ( <b>section 4(1)(k)</b> ).....	12
Public registries ( <b>section 4(1)(l)</b> ).....	13
Records of elected officials of local public bodies ( <b>section 4(1)(m)</b> ).....	14

Personal records of appointed or elected members of the governing body of a local public body ( <b>section 4(1)(n)</b> ).....	15
Personal or constituency records of a member of the Executive Council ( <b>section 4(1)(o)</b> ) .....	16
Records of the Speaker or an MLA that are in the custody or control of the Legislative Assembly Office ( <b>section 4(1)(p)</b> ) .....	16
Correspondence of Ministers, MLAs and agency heads ( <b>section 4(1)(q)</b> ).....	16
Alberta Treasury Branch records ( <b>section 4(1)(r)</b> ) .....	17
Credit union records ( <b>section 4(1)(s)</b> ) .....	17
Credit union records respecting loans assumed by the Credit Union Deposit Guarantee Corporation ( <b>section 4(1)(t)</b> ) .....	18
Health information of a public body that is a custodian under the <i>Health Information Act</i> ( <b>section 4(1)(u)</b> ) .....	18
Records excluded from Part 1 only .....	18
Briefing books ( <b>section 6(4)</b> ) .....	18
Records relating to an audit by the Chief Internal Auditor of Alberta ( <b>section 6(7)</b> ) .....	19
Accounting for excluded records.....	20
1.6 Relationship to Other Acts .....	20
Paramountcy .....	20
<i>Copyright Act</i> .....	21
<b>2. Administration of the FOIP Act.....</b>	<b>23</b>
Overview .....	23
2.1 Public Body – Roles and Responsibilities.....	23
Head of a public body .....	23
FOIP Coordinator .....	24
Program administrators .....	25
Public relations or communications .....	26
Records and information management .....	26
2.2 Delegation of FOIP Responsibilities.....	27
2.3 Province-wide Administration of the Act .....	29
Minister responsible for the <i>FOIP Act</i> .....	29
Access and Privacy, Service Alberta.....	29
Key departments.....	30
Information and Privacy Commissioner.....	30
2.4 Routine Disclosure and Active Dissemination of Information .....	31
Routine disclosure .....	31
Answers to particular questions.....	32
Specifying categories of records for routine release.....	32
Active dissemination .....	33
Practices for routine disclosure and active dissemination .....	33
Review information holdings .....	33
Establish a coordinating committee.....	34
Review requests for information .....	34
Delegate authority .....	34



Create new records .....	35
Special conditions for personal information .....	35
2.5 Exercise of Individual Rights by Authorized Representatives .....	36
Deceased individual ( <b>section 84(1)(a)</b> ) .....	36
Guardian or trustee ( <b>section 84(1)(b)</b> ) .....	36
Personal directive ( <b>section 84(1)(c)</b> ) .....	36
Power of attorney ( <b>section 84(1)(d)</b> ) .....	37
Minors ( <b>section 84(1)(e)</b> ) .....	37
Written authorization ( <b>section 84(1)(f)</b> ) .....	39
2.6 Notice and Manner of Giving Notice .....	39
Third party notices .....	40
2.7 Directories .....	41
Directory of public bodies ( <b>section 87(1)</b> ) .....	41
Directory of personal information banks ( <b>section 87.1(5)</b> ) .....	41
2.8 Accessing Manuals and Guidelines .....	42
2.9 Disclosure to the Commissioner by a Public Body Employee .....	43
2.10 Liability .....	44
Protection from liability .....	44
2.11 Offences and Penalties .....	44
<b>3. Access to Records .....</b>	<b>47</b>
Overview .....	47
FOIP Request-Handling Process (flowchart) .....	48
3.1 Who has a Right of Access .....	47
3.2 Receiving a FOIP Request .....	49
Form of the request .....	49
Alternative methods of requesting access .....	49
Duty to assist applicant ( <b>section 10(1)</b> ) .....	50
Providing information necessary for the exercise of rights under the Act .....	51
Clarifying the request .....	51
Performing an adequate search for records .....	52
Responding to the applicant .....	53
Acknowledging receipt of request .....	53
Continuing requests ( <b>section 9</b> ) .....	54
Request for access to personal information about an applicant .....	55
Request for access to personal information that includes health information .....	55
For public bodies that are not custodians under the <i>Health Information Act</i> .....	55
For public bodies that are custodians under the <i>Health Information Act</i> .....	55
Authorization to disregard requests ( <b>section 55</b> ) .....	57
Repetitious or systematic requests .....	57
Frivolous or vexatious requests .....	58
Effect of an authorization request on time limits .....	59
Clarifying requests .....	59

Release of information outside the FOIP process.....	60
Narrowing a request .....	60
Changing the scope.....	60
Documenting and tracking requests .....	60
Transferring a request.....	61
Transfer procedure ( <b>section 15(1)</b> ).....	62
Transfer of a request for correction ( <b>section 37</b> ).....	63
Conditions of transfer ( <b>sections 15(2)</b> and <b>37(2)</b> ) .....	63
Consultation .....	63
3.3 Response time limits .....	64
Deemed refusal ( <b>section 11(2)</b> ).....	64
Time limit extensions ( <b>section 14</b> ).....	64
Limits on extensions.....	66
Notification ( <b>section 14(4)</b> ).....	67
Impact of third party notice on response times.....	67
Day of response .....	68
3.4 Processing a FOIP Request – Search and Retrieval .....	68
Receipt of a request .....	68
Locating, retrieving and copying records.....	69
Disposition of records.....	70
Preliminary assessment .....	71
Notices.....	72
3.5 Assessing Fees .....	72
Fees for general records .....	73
Fees for personal information.....	74
Fee estimates .....	75
Deposits and payment of fees.....	76
Excusing or waiving fees .....	77
Grounds for excusing fees.....	78
Applicant cannot afford to pay ( <b>section 93(4)(a)</b> ).....	78
Other reasons why it is fair to excuse payment ( <b>section 93(4)(a)</b> ).....	78
Record relates to a matter of public interest ( <b>section 93(4)(b)</b> ) .....	79
3.6 Abandonment of Requests .....	81
3.7 Processing a FOIP Request – Reviewing and Preparing Records for Disclosure .....	82
Line-by-line review of records .....	82
Documentation .....	82
Reviewer’s recommendations.....	82
Creating a new record.....	83
Responsive information.....	84
Severing information.....	85
Information that must or may be severed .....	86
Procedures .....	86
Indication of severing.....	87
Maintenance of copies.....	88

3.8 Responding to an Applicant .....	88
Model responses .....	89
Record does not exist .....	89
Access is granted .....	90
Excluded records .....	91
Access denied .....	91
Refusal to confirm or deny existence of record .....	92
Request file .....	92
3.9 Completion of Request and Closure of Request File .....	92
Completion of request .....	92
Closure of file .....	93
Retention of file .....	94
<b>4. Exceptions to the Right of Access .....</b>	<b>95</b>
Overview .....	95
4.1 Introduction .....	95
Mandatory and discretionary exceptions .....	96
Exercise of discretion .....	97
Harms test .....	99
Other tests .....	99
Application of exceptions .....	99
Claiming additional exceptions .....	100
Time limitation on the application of certain exceptions .....	100
4.2 Disclosure Harmful to Business Interests of a Third Party .....	101
Type of information ( <b>section 16(1)(a)</b> ) .....	101
Supplied in confidence ( <b>section 16(1)(b)</b> ) .....	104
Effect on business interests ( <b>section 16(1)(c)</b> ) .....	106
Harm significantly the competitive position of a third party ( <b>section 16(1)(c)(i)</b> ) .....	106
Interfere significantly with the negotiating position of a third party ( <b>section 16(1)(c)(i)</b> ) .....	107
Result in similar information no longer being supplied to the public body ( <b>section 16(1)(c)(ii)</b> ) .....	107
Result in undue financial loss or gain to any person or organization ( <b>section 16(1)(c)(iii)</b> ) .....	108
Reveal labour relations information ( <b>section 16(1)(c)(iv)</b> ) .....	108
Tax information ( <b>section 16(2)</b> ) .....	109
When the exception does not apply ( <b>section 16(3)</b> ) .....	110
If the third party consents ( <b>section 16(3)(a)</b> ) .....	110
If an enactment of Alberta or Canada authorizes or requires disclosure ( <b>section 16(3)(b)</b> ) .....	111
If the information relates to a non-arm's length transaction between a public body and another party ( <b>section 16(3)(c)</b> ) .....	111
If the information is in a record in the archives of a public body and has been in existence for 50 years or more ( <b>section 16(3)(d)</b> ) .....	111
Application of exception .....	111
Figure 1: Section 16 – Disclosure Harmful to Business Interests of a Third Party .....	112

4.3 Disclosure Harmful to Personal Privacy .....	113
Definition of personal information .....	113
Exception for personal information ( <b>section 17(1)</b> ) .....	113
Disclosure not an unreasonable invasion of a third party's privacy ( <b>section 17(2)</b> ) .....	113
Consent to or request for disclosure ( <b>section 17(2)(a)</b> ) .....	114
Compelling circumstances affecting anyone's health or safety ( <b>section 17(2)(b)</b> ) .....	115
Act of Alberta or Canada authorizes or requires disclosure ( <b>section 17(2)(c)</b> ) .....	115
Classification, salary range, discretionary benefits or employment responsibilities of public officials ( <b>section 17(2)(e)</b> ) .....	115
Contracts to supply goods and services to a public body ( <b>section 17(2)(f)</b> ) .....	118
Licence, permit or similar discretionary benefit relating to a commercial or professional activity or to real property ( <b>section 17(2)(g)</b> ) .....	118
Discretionary benefit of a financial nature ( <b>section 17(2)(h)</b> ) .....	119
Individual dead for 25 years or more ( <b>section 17(2)(i)</b> ) .....	120
Disclosure not contrary to the public interest ( <b>section 17(2)(j)</b> and <b>17(3)</b> ) .....	120
Enrolment in a school, or in a program of a post-secondary educational body ( <b>section 17(2)(j)(i)</b> ) .....	121
Attendance at or participation in a public event or public activity ( <b>section 17(2)(j)(iii)</b> ) .....	122
Receipt of an honour or award granted by or through a public body ( <b>section 17(2)(j)(iv)</b> ) .....	122
Request for non-disclosure of personal information ( <b>section 17(3)</b> ) .....	123
Presumption of unreasonable invasion of privacy ( <b>section 17(4)</b> ) .....	123
Medical, psychiatric or psychological information ( <b>section 17(4)(a)</b> ) .....	124
Information that is an identifiable part of a law enforcement record ( <b>section 17(4)(b)</b> ) .....	124
Information that relates to eligibility for income assistance or social service benefits ( <b>section 17(4)(c)</b> ) .....	125
Employment or educational history ( <b>section 17(4)(d)</b> ) .....	126
Personal information collected on a tax return or gathered for the purpose of collecting a tax ( <b>section 17(4)(e)</b> ) .....	127
Bank account and credit card information ( <b>section 17(4)(e.1)</b> ) .....	127
Personal recommendations or evaluations, character references or personnel evaluations ( <b>section 17(4)(f)</b> ) .....	127
Name of individual with other personal information or that would reveal other personal information ( <b>section 17(4)(g)</b> ) .....	128
Racial or ethnic origin or religious or political beliefs or associations ( <b>section 17(4)(h)</b> ) .....	128
Circumstances relevant to the determination of unreasonable invasion of privacy ( <b>section 17(5)</b> ) .....	129
Circumstances weighing in favour of disclosure .....	130
Public scrutiny ( <b>section 17(5)(a)</b> ) .....	130
Public health, safety and protection of the environment ( <b>section 17(5)(b)</b> ) .....	130
Determination of an applicant's rights ( <b>section 17(5)(c)</b> ) .....	131
Research on or validation of the claims, disputes or grievances of aboriginal people ( <b>section 17(5)(d)</b> ) .....	132
Circumstances weighing against disclosure .....	132
Exposure to financial or other harm ( <b>section 17(5)(e)</b> ) .....	132

Personal information supplied in confidence ( <b>section 17(5)(f)</b> ).....	132
Inaccurate or unreliable personal information ( <b>section 17(5)(g)</b> ).....	134
Unfair damage to reputation ( <b>section 17(5)(h)</b> ) .....	134
Other circumstances to consider.....	134
Personal information originally provided by the applicant ( <b>section 17(5)(i)</b> ) .....	134
Existence of record ( <b>section 12(2)(b)</b> ).....	135
Application of exception .....	135
Figure 2: Section 17 – Disclosure Harmful to Personal Privacy .....	136
4.4 Disclosure Harmful to Individual or Public Safety .....	137
Harm to another's health or safety or interference with public safety.....	137
Harm to the applicant's health or safety.....	138
Information about individual health or safety supplied in confidence .....	139
Existence of record.....	139
Application of exception .....	139
Figure 3: Section 18 – Disclosure Harmful to Individual or Public Safety .....	140
4.5 Confidential Evaluations.....	141
Confidential evaluations for employment, contracts or other benefits ( <b>section 19(1)</b> ).....	141
Confidential information for employee evaluation ( <b>section 19(2) and (3)</b> ) .....	142
Information provided in confidence .....	143
Application of exception .....	143
Figure 4: Section 19 – Confidential Evaluations.....	144
4.6 Disclosure Harmful to Law Enforcement .....	145
Definition of law enforcement.....	145
Exception for law enforcement information.....	147
Harm a law enforcement matter ( <b>section 20(1)(a)</b> ).....	148
Prejudice the defence of Canada or of any foreign state allied to or associated with Canada ( <b>section 20(1)(b)</b> ).....	148
Disclose activities suspected of constituting threats to the security of Canada ( <b>section 20(1)(b.1)</b> ).....	149
Harm the effectiveness of investigative techniques and procedures ( <b>section 20(1)(c)</b> ) ....	150
Reveal the identity of a confidential source ( <b>section 20(1)(d)</b> ).....	150
Reveal criminal intelligence relating to organized criminal activities ( <b>section 20(1)(e)</b> ).....	151
Interfere with or harm an ongoing or unsolved investigation ( <b>section 20(1)(f)</b> ).....	152
Reveal information relating to the exercise of prosecutorial discretion ( <b>section 20(1)(g)</b> ) .....	152
Deprive of the right to a fair trial or impartial adjudication ( <b>section 20(1)(h)</b> ).....	153
Reveal a record confiscated by a peace officer ( <b>section 20(1)(i)</b> ).....	153
Facilitate escape from custody ( <b>section 20(1)(j)</b> ).....	154
Facilitate the commission of an unlawful act ( <b>section 20(1)(k)</b> ) .....	154
Reveal technical information relating to weapons ( <b>section 20(1)(l)</b> ).....	154
Harm the security of property and systems ( <b>section 20(1)(m)</b> ) .....	155
Reveal information in a confidential correctional record ( <b>section 20(1)(n)</b> ) .....	155
Exposure to civil liability or harm to the proper custody or supervision of an individual ( <b>section 20(3)</b> ).....	156
Exposure to civil liability ( <b>section 20(3)(a)</b> ).....	156



Harm to the proper custody or supervision of an individual under the control of a correctional authority ( <b>section 20(3)(b)</b> ) .....	156
Disclosure is an offence under an Act of Canada ( <b>section 20(4)</b> ) .....	157
When the exception does not apply ( <b>section 20(5)</b> ) .....	157
Completed investigations ( <b>section 20(6)</b> ) .....	158
Existence of record ( <b>section 12(2)</b> ) .....	158
Application of exception .....	159
Figure 5: Section 20 – Disclosure Harmful to Law Enforcement .....	160
4.7 Disclosure Harmful to Intergovernmental Relations .....	161
Consultation .....	161
Harm to intergovernmental relations ( <b>section 21(1)(a)</b> ) .....	161
Disclosure of information ( <b>section 21(2)</b> ) .....	163
Information supplied in confidence ( <b>section 21(1)(b)</b> ) .....	163
Disclosure of information ( <b>section 21(3)</b> ) .....	164
Time limitation ( <b>section 21(4)</b> ) .....	164
Application of exception .....	164
Figure 6: Section 21 – Disclosure Harmful to Intergovernmental Relations .....	165
4.8 Cabinet and Treasury Board Confidences .....	166
Reveal the substance of deliberations ( <b>section 22(1)</b> ) .....	167
When the exception does not apply .....	168
Information in a record in existence for 15 years or more ( <b>section 22(2)(a)</b> ) .....	168
Information in a record of a decision made by Executive Council or any of its committees on an appeal ( <b>section 22(2)(b)</b> ) .....	169
Background facts ( <b>section 22(2)(c)</b> ) .....	169
Application of exception .....	170
Figure 7: Section 22 – Cabinet and Treasury Board Confidences .....	171
4.9 Local Public Body Confidences .....	172
Draft resolution, bylaw or other legal instrument ( <b>section 23(1)(a)</b> ) .....	172
Substance of deliberations of <i>in camera</i> meetings ( <b>section 23(1)(b)</b> ) .....	173
When the exception does not apply .....	175
Application of exception .....	175
Figure 8: Section 23 – Local Public Body Confidences .....	176
4.10 Advice from Officials .....	177
Classes of information to which section 24(1) may apply .....	177
Advice, proposals, recommendations, analyses or policy options ( <b>section 24(1)(a)</b> ) .....	178
Consultations or deliberations ( <b>section 24(1)(b)</b> ) .....	180
Positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations ( <b>section 24(1)(c)</b> ) .....	181
Plans relating to the management of personnel or administration of the public body that have not yet been implemented ( <b>section 24(1)(d)</b> ) .....	181
Contents of draft legislation, regulations and orders ( <b>section 24(1)(e)</b> ) .....	182
Contents of agendas or minutes of meetings of the governing body of a designated public body ( <b>section 24(1)(f)</b> ) .....	182
Pending policy and budgetary decisions ( <b>section 24(1)(g)</b> ) .....	182
Formal research or audit reports that are incomplete ( <b>section 24(1)(h)</b> ) .....	183

When the exception does not apply .....	183
Information in existence 15 years or more ( <b>section 24(2)(a)</b> ).....	183
Statements of the reasons for decisions made in the exercise of a discretionary power or an adjudicative function ( <b>section 24(2)(b)</b> ) .....	184
Results of product or environmental testing ( <b>section 24(2)(c)</b> ).....	184
Statistical surveys ( <b>section 24(2)(d)</b> ) .....	185
Results of background scientific or technical research in connection with the formulation of a policy proposal ( <b>section 24(2)(e)</b> ) .....	185
Instructions or guidelines issued to public body officers or employees ( <b>section 24(2)(f)</b> ) .....	185
Substantive rule or policy statement used to interpret legislation or administer a public body program or activity ( <b>section 24(2)(g)</b> ) .....	186
Records relating to an audit by the Chief Internal Auditor of Alberta ( <b>section 24(2.1)</b> ) .....	186
Application of exceptions.....	186
Figure 9: Section 24 – Advice from Officials .....	187
4.11 Disclosure Harmful to Economic and Other Interests of a Public Body.....	188
Harms test.....	188
Types of information .....	189
Trade secrets ( <b>section 25(1)(a)</b> ) .....	190
Financial, commercial, scientific, technical or other information where there is a proprietary interest ( <b>section 25(1)(b)</b> ) .....	190
Financial loss, prejudice to competitive position, or interfere with negotiations ( <b>section 25(1)(c)</b> ) .....	191
Research information where employee or public body could be deprived of priority of publication ( <b>section 25(1)(d)</b> ) .....	193
When the exception does not apply .....	193
Applying the exception .....	193
Figure 10: Section 25 – Disclosure Harmful to Economic and Other Interests of a Public Body or the Government of Alberta.....	194
4.12 Testing Procedures.....	195
4.13 Privileged Information .....	196
Indicators.....	196
Privileged information.....	197
Legal privilege ( <b>section 27(1)(a)</b> ) .....	197
Solicitor–client privilege .....	197
Litigation privilege .....	198
Common interest privilege.....	199
Parliamentary privilege.....	199
Police informer privilege .....	199
Case-by-case privilege.....	200
Case-by-case privilege applied to Crown records (sometimes called Crown privilege).....	200
Case-by-case privilege applied to private records .....	200
Settlement negotiation privilege .....	201
Statutory privilege .....	201

Information relating to the provision of legal services ( <b>section 27(1)(b)</b> ) .....	201
Information relating to the provision of advice or other services ( <b>section 27(1)(c)</b> ).....	202
Privileged information of a third party ( <b>section 27(2)</b> ) .....	202
Waiver of privilege.....	203
Exercise of discretion under <b>section 27</b> .....	204
Severing of information from privileged records .....	204
Applying the exception .....	204
Figure 11: Section 27 – Privileged Information .....	205
4.14 Disclosure Harmful to Historic Resources or Vulnerable Forms of Life.....	206
Historic resources ( <b>section 28(a)</b> ).....	206
Rare, endangered, threatened or vulnerable forms of life ( <b>section 28(b)</b> ) .....	206
4.15 Information that is or will be Available to the Public .....	207
Readily available to the public ( <b>section 29(1)(a)</b> ).....	207
Available for purchase by the public ( <b>section 29(1)(a.1)</b> ) .....	207
To be published or released within 60 days ( <b>section 29(1)(b)</b> ).....	207
Notification of applicant ( <b>section 29(2)</b> ).....	208
If information is not published or released ( <b>section 29(3)</b> ).....	209
<b>5. Third Party Notice .....</b>	<b>211</b>
Overview.....	211
5.1 When to Give Third Party Notice .....	211
Notice <i>must</i> be given under <b>section 30</b> .....	211
Notice <i>may</i> be given under <b>section 30</b> .....	212
Notice requirement in <b>section 30</b> does not apply .....	213
<b>Section 30</b> not relevant.....	214
5.2 Initiating the Third Party Notice Process .....	214
Notice where practicable and as soon as practicable.....	214
5.3 Time Limits.....	215
Time limits under <b>sections 30 and 31</b> .....	215
Effect of time limits.....	216
Time limit extensions for complex requests.....	216
Manner of giving notice ( <b>section 83</b> ).....	217
5.4 Notice to a Third Party .....	218
Content of third party notice.....	218
5.5 Notice to Applicant .....	219
5.6 Response from Third Party .....	219
Consent .....	220
Representations opposing disclosure.....	220
Non-response.....	220
5.7 Decision by Public Body and Notice of Decision.....	221
When a public body decides to grant access to the record .....	221
Notice to applicant.....	221
Notice to third party.....	221



When a public body decides to deny access to the record.....	222
Notice to applicant.....	222
Notice to third party.....	222
Figure 12: Sections 16 and 17 – Third Party Notice .....	223
<b>6. Disclosure in the Public Interest .....</b>	<b>225</b>
Overview.....	225
6.1 When Disclosure is Required.....	225
Information to which <b>section 32</b> applies .....	225
Disclosure without delay .....	226
6.2 Nature of Disclosure .....	226
Records and information .....	226
Disclosure to the public .....	227
Disclosure to an affected group .....	227
Disclosure to any person, including an applicant .....	227
6.3 Public Interest.....	227
Information to be disclosed .....	227
Disclosure of information about a risk of significant harm to the environment or to public health and safety ( <b>section 32(1)(a)</b> ) .....	228
Disclosure of information clearly in the public interest ( <b>section 32(1)(b)</b> ).....	228
Determination of public interest.....	229
Duty to disclose information under <b>section 32</b> .....	230
6.4 Notification... ..	230
Notification prior to disclosure.....	230
Notice of disclosure.....	231
6.5 Review .....	231
<b>7. Protection of Privacy .....</b>	<b>233</b>
Overview.....	233
Privacy principles.....	233
7.1 Collection of Personal Information .....	235
Authority for collection of personal information .....	235
Authorized by an enactment ( <b>section 33(a)</b> ) .....	236
For the purposes of law enforcement ( <b>section 33(b)</b> ) .....	237
Relates directly to and is necessary for an operating program or activity ( <b>section 33(c)</b> ) .....	237
Review of collection practices.....	239
Unsolicited Information .....	239
7.2 Manner of Collection .....	240
Direct collection .....	240
Exceptions to direct collection .....	240
Another method of collection is authorized ( <b>section 34(1)(a)</b> ) .....	240
Information may be disclosed under Division 2 of Part 2 of the Act ( <b>section 34(1)(b)</b> ) ..	241
Information is collected in a health or safety emergency ( <b>section 34(1)(c)</b> ).....	242

Information is about a designated emergency contact ( <b>section 34(1)(d)</b> ) .....	242
Information is collected to determine suitability for an honour or award ( <b>section 34(1)(e)</b> ).....	242
Information is collected from published or other public sources for fund-raising ( <b>section 34(1)(f)</b> ).....	243
Information is collected for the purpose of law enforcement ( <b>section 34(1)(g)</b> ) .....	243
Information is collected for the purpose of collecting a fine or debt ( <b>section 34(1)(h)</b> ) ...	244
Information concerns the history, release or supervision of an individual under the control of a correctional authority ( <b>section 34(1)(i)</b> ).....	244
Information is collected for use in the provision of legal services to the Government of Alberta or a public body ( <b>section 34(1)(j)</b> ).....	245
Information is necessary to determine eligibility to participate in a program or receive a benefit, product or service ( <b>section 34(1)(k)(i)</b> ) .....	245
Information is necessary to verify eligibility to participate in a program or receive benefit, product or service ( <b>section 34(1)(k)(ii)</b> ).....	245
Information is collected by the Public Trustee or the Public Guardian ( <b>section 34(1)(l)</b> ) .....	246
Information is collected for the purpose of enforcing a maintenance order ( <b>section 34(1)(m)</b> ) .....	246
Information is collected to manage or administer personnel of the public body ( <b>section 34(1)(n)</b> ) .....	247
Information is collected to assist in researching or validating the claims, disputes or grievances of aboriginal people ( <b>section 34(1)(o)</b> ) .....	248
Notification ( <b>section 34(2)</b> ).....	248
Exception to notification ( <b>section 34(3)</b> ) .....	250
7.3 Accuracy and Retention .....	250
Accuracy and completeness ( <b>section 35(a)</b> ) .....	251
Retention ( <b>section 35(b)</b> ) .....	252
7.4 Correction of Personal Information.....	253
Right to request correction of personal information.....	253
How a request is made.....	255
When a correction is made .....	255
When a correction is refused ( <b>section 36(3)</b> ) .....	256
Annotating a request for correction.....	256
Notification of other public bodies and third parties ( <b>section 36(4), (5) and (6)</b> ) .....	257
Time limits ( <b>section 36(7)</b> ) .....	258
Transfer of requests for correction ( <b>section 37</b> ).....	259
7.5 Protection of Personal Information .....	259
7.6 Use of Personal Information .....	260
For the original or a consistent purpose ( <b>section 39(1)(a)</b> ) .....	260
With the consent of the individual ( <b>section 39(1)(b)</b> ).....	261
For a purpose for which the information may be disclosed to a public body under section 40, 42 or 43 ( <b>section 39(1)(c)</b> ) .....	263
Information in alumni records of a post-secondary educational body for fund-raising ( <b>section 39(2) and (3)</b> ).....	263
Limit on use of personal information ( <b>section 39(4)</b> ) .....	264

7.7 Disclosure of Personal Information.....	264
Disclosure in accordance with Part 1 of the Act ( <b>section 40(1)(a)</b> ).....	267
Disclosure that would not be an unreasonable invasion of a third party's privacy under section 17 ( <b>section 40(1)(b)</b> ).....	267
Disclosure for original or consistent purpose ( <b>section 40(1)(c)</b> ).....	268
Disclosure with consent ( <b>section 40(1)(d)</b> ).....	269
Disclosure to comply with an enactment of Alberta or Canada or with a treaty, arrangement or agreement under an enactment of Alberta or Canada ( <b>section 40(1)(e)</b> ).....	270
Disclosure that is authorized or required by an enactment of Alberta or Canada ( <b>section 40(1)(f)</b> ).....	272
Disclosure to comply with a subpoena, warrant or order ( <b>section 40(1)(g)</b> ).....	273
Disclosure to an officer or employee of the public body, or to a member of Executive Council ( <b>section 40(1)(h)</b> ).....	274
Disclosure for a common or integrated program or service ( <b>section 40(1)(i)</b> ).....	276
Disclosure to enforce a legal right of the Government of Alberta or a public body ( <b>section 40(1)(j)</b> ).....	277
Disclosure to collect a fine or debt or to make a payment ( <b>section 40(1)(k)</b> ).....	277
Disclosure to determine or verify suitability or eligibility for a program or benefit ( <b>section 40(1)(l)</b> ).....	279
Disclosure for audit purposes ( <b>section 40(1)(m)</b> ).....	279
Disclosure to a Member of the Legislative Assembly ( <b>section 40(1)(n)</b> ).....	280
Disclosure to a representative of a bargaining agent ( <b>section 40(1)(o)</b> ).....	281
Disclosure for archival purposes ( <b>section 40(1)(p)</b> ).....	282
Disclosure to assist law enforcement ( <b>section 40(1)(q)</b> ).....	282
Disclosure among law enforcement agencies ( <b>section 40(1)(r)</b> ).....	284
Disclosure in case of injury, illness or death ( <b>section 40(1)(s)</b> ).....	284
Disclosure in accordance with section 42 or 43 ( <b>section 40(1)(t)</b> ).....	284
Disclosure to an expert for the purposes of section 18(2) ( <b>section 40(1)(u)</b> ).....	285
Disclosure for use in a court or quasi-judicial proceeding ( <b>section 40(1)(v)</b> ).....	285
Disclosure to a place of lawful detention ( <b>section 40(1)(w)</b> ).....	286
Disclosure for the management or administration of personnel ( <b>section 40(1)(x)</b> ).....	286
Disclosure to enforce maintenance orders ( <b>section 40(1)(y)</b> ).....	287
Disclosure to an officer of the Legislature ( <b>section 40(1)(z)</b> ).....	288
Disclosure for supervision of an individual by a correctional authority ( <b>section 40(1)(aa)</b> ).....	288
Disclosure of information available to the public ( <b>section 40(1)(bb)</b> ).....	289
Disclosure of business contact information ( <b>section 40(1)(bb.1)</b> ).....	290
Disclosure to a relative of a deceased person ( <b>section 40(1)(cc)</b> ).....	290
Disclosure to the legal representative of an inmate ( <b>section 40(1)(dd)</b> ).....	292
Disclosure to avert imminent danger to health or safety ( <b>section 40(1)(ee)</b> ).....	292
Disclosure for administration of the <i>Motor Vehicle Accident Claims Act</i> ( <b>section 40(1)(ff)</b> ).....	293
Disclosure of alumni records for fund-raising purposes ( <b>section 40(2)</b> ).....	293
Disclosure of teaching and course evaluations ( <b>section 40(3)</b> ).....	293
Extent of disclosure ( <b>section 40(4)</b> ).....	294
7.8 Consistent Purposes .....	294

Examples of a consistent purpose.....	295
Evaluation of a program .....	295
Verification of ownership.....	295
Expansion of a program.....	295
7.9 Disclosure for Research or Statistical Purposes .....	296
Individually identifiable information .....	297
Record linkage ( <b>section 42(b)</b> ) .....	297
Approval of conditions ( <b>section 42(c)</b> ) .....	298
Agreement to comply with approved conditions ( <b>section 42(d)</b> ).....	299
7.10 Disclosure of Information in Archives.....	300
The Provincial Archives of Alberta or the archives of a public body .....	300
Disclosure of personal information ( <b>section 43(1)(a)</b> ).....	300
Disclosure of information other than personal information ( <b>section 43(1)(b)</b> ).....	301
Effect of other Acts .....	302
7.11 Record of Purposes ( <b>section 87(4)</b> ) .....	303
<b>8. Records and Information Management.....</b>	<b>305</b>
Overview.....	305
8.1 Scope.....	305
8.2 Powers of the Commissioner.....	306
8.3 Records and Information Management Principles .....	306
Information is an important asset of the organization .....	306
The management of information is planned .....	307
A life-cycle management approach is adopted.....	307
All records are included .....	307
Accountability is assigned.....	307
8.4 Records and Information Management Policy Components.....	308
Managing recorded information throughout its life cycle .....	308
Establishing and maintaining a records system.....	308
Establishing and maintaining a directory of personal information banks .....	309
Creating, maintaining and using records .....	309
Scheduling and disposing of recorded information .....	309
Securely disposing of personal information .....	310
Securely disposing of electronic records.....	311
Disposing of transitory records .....	311
Organizing, storing and protecting recorded information .....	312
Organizing and storing electronic records.....	313
Including routine disclosure practices and privacy requirements in the planning and design of electronic information systems .....	313
Managing recorded information in contracting .....	314
8.5 Records Issues Relating to Access Requests.....	314
Ability to find records .....	314
Adequate documentation.....	316

Controls over disposition.....	316
Ability to routinely disclose records outside the FOIP process.....	316
<b>9. Privacy Compliance .....</b>	<b>319</b>
Overview.....	319
9.1 Privacy Compliance Reviews.....	319
Protection of personal information analysis .....	320
Authority for collection ( <b>section 33</b> ).....	320
Manner of collection ( <b>section 34(1)</b> ) .....	320
Notification of collection ( <b>section 34(2)</b> ).....	321
Accuracy of personal information ( <b>section 35(a)</b> ).....	322
Correction of personal information ( <b>section 36</b> ).....	322
Directories of Personal Information Banks ( <b>section 87.1</b> ).....	323
Retention of personal information ( <b>section 35(b)</b> ).....	323
Protection of personal information ( <b>section 38</b> ).....	324
Use ( <b>section 39</b> ) .....	325
Disclosure ( <b>section 40</b> ) .....	326
Research or statistical purposes ( <b>section 42</b> ) .....	326
Data sharing and data matching .....	326
9.2 Privacy Considerations when Planning New Programs, Administrative Practices or Information Systems .....	327
9.3 Privacy Impact Assessments .....	328
When is a privacy impact assessment needed? .....	328
What is the process for a PIA? .....	329
Consider establishing a PIA development team .....	329
Consider when to start the process .....	330
Determine who will approve the PIA internally .....	330
Consider whether public consultation is needed .....	330
Understand the role of the Office of the Information and Privacy Commissioner .....	330
Privacy impact assessment questionnaire.....	331
Part A: Organizational Privacy Management .....	332
Part B: Project Privacy Management.....	332
9.4 Reviewing Forms and Other Collection Instruments .....	333
Notification.....	334
Optional practices.....	334
Collecting information on-line .....	335
9.5 Developing a Security Policy .....	335
Basic attributes of a comprehensive security policy .....	336
Authority.....	336
What needs to be safeguarded .....	337
Sensitive information.....	337
Threat and risk assessments.....	337
Types of safeguards.....	338
Breaches, sanctions and review .....	339



Security in contracting.....	339
9.6 Conducting Threat and Risk Assessments .....	340
Components of a threat and risk assessment .....	340
Determine what needs to be protected and what level of protection is required .....	340
Define the threats to protect against .....	341
Estimate the likelihood of the threat scenario occurring and the potential impact or injury that could result.....	342
Assess whether current or proposed security measures are appropriate to reduce the risk .....	342
Identify how to manage the residual risk after implementing safeguards .....	342
9.7 Privacy Considerations for Data Sharing and Data Matching.....	343
Data sharing.....	343
Data matching .....	343
Preliminary assessment.....	345
Cost-benefit analysis.....	346
Notification of the Information and Privacy Commissioner.....	346
Approval.....	347
Public notification of a matching program .....	347
Special conditions relating to the disclosure of information for matching programs .....	347
Verification process.....	348
Security.....	348
Retention and disposition .....	348
<b>10. Information and Privacy Commissioner.....</b>	<b>349</b>
Overview.....	349
10.1 Appointment .....	349
10.2 Mandate and General Powers.....	349
10.3 Monitoring Role.....	351
10.4 Provision of Advice .....	352
10.5 Disclosure to the Commissioner .....	352
10.6 Powers, Privileges and Immunities.....	353
Power under the <i>Public Inquiries Act</i> .....	353
Power to compel production of records.....	353
Power to disregard requests.....	354
Statements provided to the Commissioner .....	354
Protection from liability .....	355
Delegation of the Commissioner's powers.....	355
10.7 Reviews.....	355
Requesting a review .....	356
Preparation for a review .....	357
Review process.....	357
Mediation .....	358
Inquiry .....	358

Refusal to conduct inquiry .....	359
Time limits for review .....	360
Burden of proof .....	360
Commissioner's Orders .....	361
10.8 Investigations .....	362
Time limits on complaints .....	364
10.9 Privacy Compliance Investigations and Audits .....	364
10.10 Judicial Review .....	364
10.11 Adjudicator Process .....	365
Figure 13: Information and Privacy Commissioner Review Process.....	367
<b>Appendix 1: Definitions .....</b>	<b>369</b>
<b>Appendix 2: Delegation and Assignment of Responsibility Tables .....</b>	<b>383</b>
2.1 Delegation Table – Provisions of the Act for which Delegation of Authority should be Considered .....	383
2.2 Administrative Responsibilities that may be Assigned .....	389
<b>Appendix 3: Model Letters .....</b>	<b>395</b>
A Acknowledgment of request.....	396
A.1 Notice of processing an access request under the <i>Health Information Act</i> .....	399
B Notification during a continuing request.....	400
C Transfer of request .....	401
D Notice regarding extension of time limit.....	402
E Fee estimate .....	404
F Abandonment of a request.....	407
G Response to access request – Granting access .....	409
H Response to access request – Access to all or part of records refused .....	411
I Response to access request – Record does not exist .....	413
J Refusal to confirm or deny existence of a record.....	414
K Letter to Speaker of the Legislative Assembly regarding parliamentary privilege .....	415
L Notice to third party under <b>section 30</b> .....	416
M Notice to applicant under <b>section 30(5)</b> .....	421
N Notice to third party regarding decision under <b>section 31</b> .....	422
O Notice to applicant regarding decision under <b>section 31</b> .....	425
P Notice to third party under <b>section 32</b> (disclosure in the public interest) .....	428
Q Notice to third party under <b>section 32</b> after disclosure of information .....	429
R Notice to third party of disclosure of personal information under <b>section 17(2)(b)</b> .....	430
S Acknowledgment of receipt of correction request .....	431
S.1 Notice of processing a request for correction or amendment under the <i>Health Information Act</i> .....	432
T Notification concerning a request for correction or annotation.....	433
U Notice to public bodies in receipt of personal information .....	435
V Initial letter to expert under <b>section 18(2)</b> .....	436
W Letter transmitting records to expert under <b>section 18(2)</b> .....	438

<b>Appendix 4: Model FOIP Request Charts.....</b>	<b>439</b>
Chart 1: Model FOIP Request (Time limit not extended).....	439
Chart 2: Model FOIP Request (Time limit extended for third party notice).....	443
<b>Appendix 5: Forms .....</b>	<b>447</b>
Request to Access Information form	
Request Statistics Report	
Transmittal Memorandum (sample)	
Access Request Processing Summary form	
Access Request Recommendation form	
Access Request Recommendation Attachment: Detailed Review of Records form	
Request to Correct Personal Information form	
Annotation to Personal Information form	
Law Enforcement Disclosure form	
Authorization of Representative form (includes Affidavit of Witness form)	
Proposal to Access Personal Information for Research or Statistical Purposes form	
Agreement for Access to Personal Information for Research or Statistical Purposes form	
Office of the Information and Privacy Commissioner – Request for Review form	
<b>Indexes:</b>	
<b><i>Freedom of Information and Protection of Privacy Act and Regulation Citations .....</i></b>	<b>449</b>
<i>Freedom of Information and Protection of Privacy Act .....</i>	451
<i>Freedom of Information and Protection of Privacy Regulation .....</i>	457
<b>Information and Privacy Commissioner's Order and Investigation Report Citations .....</b>	<b>459</b>
<b>Words and Phrases Defined or Discussed.....</b>	<b>465</b>
<b>Subject. ....</b>	<b>473</b>







# 1.

## PURPOSES AND SCOPE OF THE FOIP ACT

### Overview

This chapter covers

- the purposes of the *Freedom of Information and Protection of Privacy Act* (the *FOIP Act*);
- the scope of the *FOIP Act*;
- the records that are subject to the *FOIP Act*;
- the meaning of custody or control of records;
- excluded records;
- records to which a paramouncy applies.

### 1.1 Purposes of the FOIP Act

The basic objectives of the *Freedom of Information and Protection of Privacy Act* (the *FOIP Act*) are

- to ensure that public bodies are open and accountable to the public by providing a right of access to records; and
- to protect the privacy of individuals by controlling the manner in which public bodies collect, use and disclose personal information.

**Section 2** of the Act sets out five purposes.

**A right of access to records.** The first purpose is to establish a right of access by any person to records in the custody or under the control of a public body, subject to limited and specific exceptions, which are set out in the Act. This right of access is the cornerstone of openness and accountability and should be taken into account when making any decision about disclosing records in response to a FOIP request.

The limited and specific exclusions and exceptions set out in the Act, and a small number of provisions of other legislation that take precedence over the Act, provide the only basis for refusing access to records and should always be interpreted with a view to giving as much access as possible to the records requested.

**Protection of personal privacy.** The second purpose is to control the manner in which a public body may collect, use and disclose the personal information of individuals. This purpose also requires public bodies to ensure that personal information that is used to make a decision about an individual is accurate and complete, that it is retained long enough to enable the individual to obtain access to it, and that it is protected and properly disposed of. These privacy protection measures are often referred to as fair information practices.

**A right of access to an individual's own personal information.** The third purpose is to create a right of access for individuals to personal information about themselves, again subject to limited and specific exceptions set out in the Act. Public bodies

should interpret the exceptions with a view to giving an individual as much access as possible to his or her own personal information.

**A right to request a correction.** The fourth purpose is to allow individuals a right to request corrections to personal information about themselves that is held by a public body.

**Independent review of decisions.** The fifth purpose is to provide for the independent review of decisions made by public bodies under the Act and for the investigation of complaints. Independent review is provided by the Information and Privacy Commissioner.

### **Scope of the Act**

The *FOIP Act* applies to all public bodies. **Section 1** of the Act contains a number of definitions that set out which bodies are and are not public bodies for the purposes of the Act. Bodies that are subject to the Act have statutory duties with regard to access to information and protection of privacy.

**Section 4** of the Act establishes which records are subject to the Act and which records are excluded. **Section 4** is discussed in detail in section 1.5 of this chapter.

### **Public body**

**Section 1(p)** A public body is defined in the Act to mean:

- a department, branch or office of the Government of Alberta;
- an agency, board, commission, corporation, office, or other body designated as a public body in the regulations (**Schedule 1** of the FOIP Regulation);
- the Executive Council Office;
- the office of a member of the Executive Council;
- the Legislative Assembly Office;
- the office of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, or the Information and Privacy Commissioner; or
- a local public body.

The *FOIP Act* came into force for public bodies other than local public bodies on October 1, 1995.

### **Local public body**

**Section 1(j)** A local public body is defined in the Act to mean:

- an educational body;
- a health care body; or
- a local government body.

### **Educational body**

**Section 1(d)** An educational body is defined in the Act to mean:

- a university as defined in the *Post-secondary Learning Act*;

- a technical institute as defined in the *Post-secondary Learning Act*;
- a public college as defined in the *Post-secondary Learning Act*;
- the Banff Centre as defined in the *Post-secondary Learning Act*;
- a board as defined in the *School Act*;
- a charter school as defined in the *School Act*; or
- a regional authority as defined in the *School Act*.

The *FOIP Act* came into force for educational bodies other than post-secondary institutions on September 1, 1998 and for post-secondary institutions on September 1, 1999.

### **Health care body**

**Section 1(g)** A health care body is defined in the Act to mean:

- the board of an approved hospital as defined in the *Hospitals Act*, other than an approved hospital that is owned and operated by a regional health authority under the *Regional Health Authorities Act*;
- the operator of a nursing home as defined in the *Nursing Homes Act*, other than a nursing home that is owned and operated by a regional health authority under the *Regional Health Authorities Act*;
- a provincial health board established under the *Regional Health Authorities Act*;
- a regional health authority under the *Regional Health Authorities Act*;
- a community health council established under the *Regional Health Authorities Act*; or
- a subsidiary health corporation as defined in the *Regional Health Authorities Act*.

As of April 1, 2009, there is one regional health authority. The name of the body corporate is Alberta Health Services and the name of the area served by the regional health authority is the Alberta Health Region.

Hospitals and nursing homes directly owned and operated by a regional health authority are part of the regional health authority, that is, Alberta Health Services. Other public hospitals and nursing homes are separate local public bodies.

The Alberta Alcohol and Drug Abuse Commission (AADAC) and the Alberta Cancer Board have been dissolved and their functions have been assumed by Alberta Health Services.

The *FOIP Act* came into force for health care bodies on October 1, 1998.

### **Local government body**

**Section 1(i)** A local government body is defined in the Act to mean:

- a municipality as defined in the *Municipal Government Act*;
- an improvement district under the *Municipal Government Act*;
- a special area as defined by the *Special Areas Act*;

- a regional services commission under Part 15.1 of the *Municipal Government Act*;
- a board established under the *Drainage Districts Act*;
- a board established under the *Irrigation Districts Act*;
- a management body established under the *Alberta Housing Act*;
- a Metis settlement established under the *Metis Settlements Act*;
- the Metis Settlements General Council established under the *Metis Settlements Act*;
- any commission, police service or policing committee as defined in the *Police Act*;
- any municipal library board, library system board, federation board or joint municipal library board established or continued under the *Libraries Act*; or
- any board, committee, commission, panel, agency or corporation that is created or owned by any of the bodies listed above and all the members or officers of which are appointed or chosen by that body.

The *FOIP Act* came into force for local government bodies on October 1, 1999.

#### **Bodies excluded from the definition of “public body”**

**Section 1(p)** specifically excludes the following from the definition of “public body” and therefore from the scope of the Act:

- the office of the Speaker of the Legislative Assembly;
- the office of a Member of the Legislative Assembly; and
- the Court of Appeal of Alberta, the Court of Queen’s Bench of Alberta and The Provincial Court of Alberta.

Since government departments are public bodies and the Executive Council Office is a public body, but the office of a Member of the Legislative Assembly is not, some records of Members of the Executive Council (Cabinet members) will fall within the scope of the Act and others will not. The records of Members of the Executive Council that relate to their duties in Cabinet and in the administration and operation of a public body are within the scope of the Act, but records that relate to their duties as MLAs are not.

**Section 1(i)** defines local government body to exclude certain agencies from the Act.

EPCOR Utilities Inc. and ENMAX Corporation and any of their subsidiaries that own a gas utility, a generating unit, transmission facility or electric distribution system, or whose primary business activity is providing electricity services, are excluded from the scope of the *FOIP Act*. However, these organizations are subject to the provisions of the *Personal Information Protection Act* for collection, use, disclosure, retention and protection of personal information inside Alberta and to the provisions of the federal *Personal Information Protection and Electronic Documents Act* for personal information that is disclosed outside Alberta.

As well, community library boards established under the *Libraries Act* are not public bodies under the Act. However, if a community library board receives assistance from a municipality or a government department, records relating to that assistance may be available from the municipality or government department.

The RCMP is not a public body under the *FOIP Act*. The RCMP is a “government institution” subject to the federal government’s *Access to Information Act* and *Privacy Act*. RCMP detachments operating as municipal police services are not local government bodies under the *FOIP Act*.

A First Nation’s Police Service is not a public body under the *FOIP Act* and is not subject to the federal government’s access and privacy legislation.

## 1.2

### Application of the Act

#### **Existing procedures for access**

The *FOIP Act* is in addition to and does not replace existing procedures for obtaining access to information or records held by public bodies (**section 3(a)**). However, any routine disclosure of personal information by public bodies must be in compliance with **Part 2** of the Act.

Routine disclosure of information is discussed in more detail in section 2.4 of Chapter 2.

#### **Archival records**

The Act does not affect access to records in the Provincial Archives of Alberta, or any other archives of a public body, if public access to the records was not restricted before the Act came into force with respect to those archives (**section 3(b)**).

If an archival institution serving a public body declared records in a certain class or date range open to public access before the public body became subject to the Act, those records may remain open to public access. There is no need for a person to make an access request under the *FOIP Act* to see these records or for the archives to apply the Act when disclosing the records.

#### **Legal proceedings**

The Act does not limit the information otherwise available by law to a party to legal proceedings (**section 3(c)**).

*Legal proceedings* are activities governed by rules of court or rules of judicial or quasi-judicial tribunals which can result in a judgment of a court or a ruling by a tribunal.

The Act does not prevent or limit the use of legal processes such as examination for discovery to gather information about a party in a lawsuit. It is relatively common for persons involved in a criminal or civil legal action to make a FOIP request to a public body for records relating to the case. Such a request should be processed as a FOIP request, applying the provisions of the Act.

If an action proceeds to discovery, or if some other legal procedure is invoked to obtain disclosure of records, the rules governing that legal procedure will apply. The access provisions of the *FOIP Act* are applicable only to requests made under the



FOIP Act and not to other legal processes. It is common to have both processes going on at the same time. See, for example, the discussion in *IPC Order 97-009*.

The provisions of the Act do not override the power of any court or tribunal in Canada to compel a witness to testify or to compel the production of documents (**section 3(d)**).

### **Disposition of records**

The Act does not prohibit the transfer, storage or destruction of a record in accordance with an enactment of Alberta or Canada, or, in the case of local public bodies, as sanctioned by a bylaw, resolution or other legal instrument by which a local public body acts (**section 3(e)**). This provision permits the orderly disposition of records by public bodies in accordance with records retention and disposition schedules. If a local public body has no bylaw, resolution or other legal instrument with respect to the transfer, storage or destruction of records, it may carry out these functions in accordance with a policy authorized by its governing body.

See Chapter 8 for more discussion on records and information management, including the effect of **section 35(b)** of the Act on the disposition of records.

---

## **1.3 Records Subject to the Act**

The Act applies to all the records *in the custody or under the control* of a public body, including court administration records (**section 4(1)**). This means that a public body does not need to have both custody and control of a record for the Act to apply to it (see *IPC Order 2000-005*).

### **Record**

**Section 1(q)** Record means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers, and any other information that is written, photographed, recorded or stored in any manner but does not include software or any mechanism that produces records (**section 1(q)**).

Any recorded information, including handwritten notes and electronic correspondence or messages, which is in the custody or control of a public body is a record for the purposes of the Act.

Despite the reference to “books” in the definition of a record, the Act does not apply to published works collected by a library of a public body in accordance with the library’s acquisition of materials policy (**section 4(1)(j.1)**).

### **Personal information**

**Section 1(n)** The Act defines personal information as recorded information about an identifiable individual, including, but not limited to

- the individual’s name, home or business address or home or business telephone number;
- the individual’s race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual’s age, sex, marital status or family status;



- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

*Biometric information* is defined in **section 1(b.1)** to mean information derived from an individual's unique, measurable characteristics. Biometric information is collected through fingerprinting, facial and voice recognition programs, iris and retinal scans and a range of other methods designed to capture individual characteristics. This type of personal information is increasingly used in law enforcement and fraud prevention, for access to premises and for computer network security. As with all types of personal information, biometric information may be collected, used and disclosed only in accordance with **Part 2** of the Act.

*Genetic information* includes an individual's DNA information. This term was added to the definition of personal information to clarify that the *FOIP Act* applies to information obtained as a result of DNA analysis. Matters concerning ownership of DNA, the collection of DNA under the federal *DNA Identification Act* and the use of DNA in a commercial context are outside the scope of the *FOIP Act*.

#### 1.4 Custody or Control

A public body has *custody* of a record when the record is in the physical possession of the public body (see *IPC Orders 2000-003* and *2000-005*).

A record is in the *possession* of a public body if the public body is physically holding or retaining the record. Some examples of records in the possession of a public body are: active records in an employee's office filing cabinet or in a central filing system on the public body's premises; inactive records in a records storage centre that may be located off the public body's premises; working papers in an employee's desk drawer; and electronic records located on an employee's computer at work.

A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

Some indicators that a record may be in the custody or under the control of a public body are as follows:

- the record was created by an officer, employee or member of the public body;
- the record was created by an outside contracted consultant for the public body;
- the record is specified in a contract as being under the control of a public body;
- the record is in the possession of the public body;
- the record is closely integrated with other records of the public body;

- the content of the record relates to the public body's mandate and functions;
- the public body has the authority to regulate the record's use and disposition;
- the public body has relied upon the record to a substantial extent; or
- a contract permits the public body to inspect, review or copy records produced, received or acquired by a contractor as a result of a contract.

(See *IPC Order 99-032*.)

In *IPC Order 99-020*, the Information and Privacy Commissioner considered whether certain records were under the control of the Auditor General. The Commissioner decided that the typewritten notes were created by the Auditor General and were under the control of that Officer. However, he decided that handwritten notations on a public body's copies of those records must be considered separate and distinct from the typewritten portions of the records. The notations changed the character of the records and provided additional information. They were neither created by the Auditor General nor in the Auditor General's custody or control.

The most common situation where a public body may have control, but not custody, of a record is in the case of contracted services. The record may have been created by and may be in the possession of the contractor, but the public body has control of the record because it relates to a service performed by the contractor on behalf of the public body. In most cases, matters of custody and control would be addressed in the contract.

For example, if a contract requires the contractor to make records available to a public body to audit the services provided or to justify the payment of contractor's invoices, the records used by the public body to monitor or inspect the delivery of the services would likely be deemed to be under its control.

Administrative records relating to the business of a contractor would not normally be considered to be under the control of a public body unless this was specifically stipulated in the contract. If a contractor deals with a subcontractor, but a public body does not exercise any rights in regard to the records relating to the work of the subcontractor, those records will not be under the control of a public body.

A fuller discussion of FOIP and contract management is found in the publication *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.



**All public bodies should ensure that their contracts and contracting practices adequately take the FOIP Act into account.**

Where a public body stores records in a records storage facility (e.g. the Alberta Records Centre for provincial government bodies), both control and custody will likely lie with the public body placing the records in the storage facility and not with the organization offering the storage service.

## 1.5 Records Excluded from the Act

### Categories of excluded records

Certain information and records in the custody or under the control of public bodies are excluded from the application of the Act. In some cases, another process is available to obtain access to these records. The exclusions are as follows.

#### ***Certain categories of information in court and judicial records***

**Section 4(1)(a)** The *FOIP Act* does not apply to information in a court file, a record of a judge of the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, or The Provincial Court of Alberta, a record of a master of the Court of Queen's Bench of Alberta, a record of a sitting or presiding justice of the peace, a judicial administration record, or a record relating to support services provided to the judges of any of the courts referred to above.

Information in a court file is not limited to the contents of the paper file accessible to the public by doing a search at the courthouse. It also includes any information taken from such a file and used to create another record, including a criminal docket (*Alberta (Attorney General) v. Krushell*, 2003 ABQB 252).

The term *judicial administration record* is defined in **section 4(3)** of the Act and appears in the **Definitions** in Appendix 1.

#### ***Draft judicial or quasi-judicial decisions***

**Section 4(1)(b)** A personal note, communication or draft decision created by or for a person who is acting in a judicial or quasi-judicial capacity is not within the scope of the Act.

A *personal note* of a member of a judicial or quasi-judicial tribunal is one intended solely for the use of the person who wrote it (see *IPC Order 99-025*).

A *person who is acting in a judicial or quasi-judicial capacity* includes any authority designated by the Lieutenant Governor in Council that is subject to the *Administrative Procedures Act*.

This exclusion also applies to communications between the members of the judicial or quasi-judicial body themselves, and between members and support staff, when these communications relate to the judicial or quasi-judicial functions of the body.

**Section 4(1)(b)** does not apply to final decisions or reasons for decision of the judicial or quasi-judicial body, although another exclusion or exception may apply to these records.

The following criteria, which are not exhaustive, should be reviewed in determining whether a body is acting in a "judicial or quasi-judicial capacity":

- Is there anything in the language in which the function is conferred or in the general context in which it is exercised which suggests that a hearing is contemplated before a decision is reached?
- Does the decision or order directly or indirectly affect the rights and obligations of persons?
- Is the adversarial process involved?

- Is there an obligation to apply substantive rules to many individual cases rather than, for example, the obligation to implement social and economic policy in a broad sense?

(See *IPC Order 99-025*.)

No one factor is decisive and it is necessary to consider the legislation under which a decision is made to determine whether the rules of natural justice apply. The nature of the issue to be decided and the importance of the decision for those affected should also be examined. Public bodies may wish to seek legal advice when making a decision as to whether a decision-maker is acting in a judicial or quasi-judicial capacity.

Examples of provincial public bodies that make quasi-judicial decisions are the Environmental Appeals Board, the Labour Relations Board and the Board of Reference. Examples at the local government level are a Subdivision and Development Appeal Board and an Assessment Review Board. Such bodies make rulings of a judicial, as opposed to an administrative, nature.

#### **Quality assurance records of health care bodies**

**Section 4(1)(c)** Quality assurance committees study, assess and evaluate the provision of health services with a view to continuous improvement. Under section 9 of the *Alberta Evidence Act*, certain records of, and documentation supplied to, quality assurance committees (as that term is defined in the *Alberta Evidence Act*) in health care bodies are not admissible as evidence in court. **Section 4(1)(c)** excludes these quality assurance records from the scope of the *FOIP Act*.

This exclusion applies only to records of quality assurance committees as defined in the *Alberta Evidence Act*, and not to other quality assurance committees established within health care bodies, and other public bodies, to monitor the quality of health services or other services.

The exclusion for the records of quality assurance committees does not extend to original medical and hospital records of a patient, even if they were supplied to a quality assurance committee. This means that health care bodies that are custodians under the *Health Information Act* would treat the medical records of individuals disclosed to a quality assurance committee as health information subject to the *Health Information Act*.

#### **Records of an officer of the Legislature**

**Section 4(1)(d)** A record that is created by or for or is in the custody or under the control of an officer of the Legislature, and relates to the exercise of that officer's functions under an Act of Alberta, is not within the scope of the *FOIP Act*.

Operational files and correspondence of the Auditor General, the Information and Privacy Commissioner, the Ethics Commissioner, the Chief Electoral Officer, and the Ombudsman are excluded from the coverage of the Act. Correspondence to and from these offices is excluded regardless of where the correspondence or files are located. This applies to letters and draft reports in the custody of a public body. Records created by employees and contractors for these officers are also excluded. (See *IPC Order 97-008*.)



The administrative files of these legislative offices, however, are subject to the Act. These include personnel information, contracts and general office management records.

**Records provided to the Ethics Commissioner**

- Section 4(1)(e)** Information is excluded if it is collected by or for the Ethics Commissioner, or is in the custody or under the control of the Ethics Commissioner, and relates to the disclosure statements of deputy ministers and other senior officers which have been deposited with the Ethics Commissioner. This provision covers records created or compiled from information provided to the Ethics Commissioner.

**Records created by or for the Ethics Commissioner**

- Section 4(1)(f)** Records are excluded if they are created by or for the Ethics Commissioner or are in the custody or under the control of the Ethics Commissioner and relate to any advice about conflicts of interest, whether or not the advice was given under the *Conflicts of Interests Act*.

**A question to be used on an examination or test**

- Section 4(1)(g)** A question to be used on an examination or test is not within the scope of the Act. This exclusion applies to questions that are to be used in the future and question banks from which questions are to be selected for future tests. The exclusion also applies to instructions and reading passages in an examination paper (*IPC Order F2002-012*). The exclusion applies to intelligence tests, but not to a subject's answers (*IPC Order F2004-015*).

The exclusion does not apply to test banks containing tests administered in the past that may be used as a source of future questions for tests.

**Teaching materials**

- Section 4(1)(h)** The Act does not apply to teaching materials of employees of a post-secondary educational body or of the post-secondary educational body itself. Nor does it apply to teaching materials of both employees and the post-secondary educational body. This exclusion is intended to ensure that the access provisions of the Act do not compromise the right to priority of publication of those responsible for the creation of post-secondary teaching materials.

*Teaching materials* include records produced or compiled for the purpose of providing systematic instruction to a person about a subject or skill and include records created or compiled to aid the instructor in imparting information or for distribution to students.

*Post-secondary educational body* means a university, a technical institute, a public college, and the Banff Centre, all as defined in the *Post-secondary Learning Act*.

**Research information of employees**

- Section 4(1)(i)** Also excluded from the scope of the *FOIP Act* is research information of an employee of a post-secondary educational body. This provision is intended to ensure that the access provisions of the Act do not compromise the right to priority of

publication or to register patents or industrial designs of those responsible for the creation of post-secondary research information.

*Research information* includes records produced or compiled as part of a research project, and include data, working papers, bibliographies and other materials used in the research process.

**Archival materials**

**Section 4(1)(j)** Material that has been deposited in the Provincial Archives of Alberta, or in the archives of a public body, by or for a person or entity other than a public body is not within the scope of the Act.

Individuals, corporations, labour unions, churches, and other groups may place collections of papers in the archives of public bodies. These materials may continue to be owned by the depositing body or may be given to the archives. These records are not subject to the Act.

For this exclusion to apply, a record must be deposited by or on behalf of a third party with no involvement by a public body except as a recipient of the record (see *IPC Order 2000-003*).

This provision also applies to records of Members of the Executive Council who held office prior to April 1, 1995, if the records relate to a term of office prior to that date and were donated to the Provincial Archives of Alberta. These records are considered to be private records. Records relating to a term of office after that date are subject to the Act.

**Published works collected by a library**

**Section 4(1)(j.1)** The *FOIP Act* does not apply to published works collected by a library of a public body in accordance with the library's acquisition of materials policy. This provision was added to the Act in 2006 in response to concerns about works being acquired by libraries from non-traditional sources. New information technologies have made it possible for individuals to "publish," and for libraries to collect and make publicly available, material that would previously have been confined to archives. This typically occurs when libraries accept donations of privately published memoirs and local histories and put them into circulation.

The Act now makes it clear that neither the access nor the privacy provisions of the Act apply to published works, but only if the library has collected those publications in accordance with an acquisitions policy. For further information on this exclusion, see FOIP Bulletin No. 18: *FOIP Amendment Act, 2006*, published by Access and Privacy, Service Alberta.

**Records relating to an ongoing prosecution**

**Section 4(1)(k)** The Act does not apply to a record relating to a prosecution, if all proceedings in respect of the prosecution have not been completed. Prosecution records are excluded until the appeal period has expired and, in a case where Crown counsel has stayed a criminal prosecution, until the one-year period from the stay has expired.

This exclusion allows for the disclosure of information during a legal proceeding to take place in accordance with the rules governing the proceeding. However, before the proceeding takes place, and after any stay or appeal period has expired, the *FOIP Act* applies to the records involved. See also Chapter 4, section 4.6 for records relating to the exercise of prosecutorial discretion.

### **Public registries**

**Section 4(1)(l)** The Act does not apply to a record made from information in:

- the Personal Property Registry;
- the office of the Registrar of Motor Vehicle Services;
- the office of the Registrar of Corporations;
- the office of the Registrar of Companies;
- a Land Titles Office;
- an office of the Director or of a district registrar as defined in the *Vital Statistics Act*; or
- a registry operated by a public body if that registry is authorized or recognized by an enactment and public access to the registry is normally permitted.

A number of public bodies are responsible for public registries that serve the public interest by maintaining records relating to a range of legal rights and duties, including the transfer of land, corporate ownership, the securing of debt, the registration of vehicles, and the licensing of drivers. These activities tend to be subject to regulatory frameworks that attempt to provide a balance between public and private interests with respect to the information contained in the particular registry.

**Section 4(1)(l)** excludes information in the listed registries from the access provisions under **Part 1** of the Act and the use and disclosure provisions under **Part 2**. This exclusion allows for the operation of other policies and procedures for access to information and the protection of personal information in registries. The Commissioner has interpreted **section 4(1)(l)** in a number of Orders.

The Commissioner considered the extent of the exclusion for registries in an Order relating to records made from information in the office of the Registrar of Motor Vehicle Services (**section 4(1)(l)(ii)**). He decided that, because the exclusion applied to records *made from* the information in the registry, the collection of information by the Registrar was *not* excluded from the *FOIP Act*. The collection of information in the first instance by Alberta Registries is subject to the Act (see *IPC Orders 2000-020, 2000-023 and 2001-029*).

For example, Vital Statistics was authorized under the *Vital Statistics Act* to collect certain prenatal information of mothers from the physician's notice of birth. The Commissioner had jurisdiction only to determine whether too much information was being collected (see *IPC Investigation Report 99-IR-001*).

A *registrar* means an officer who has the custody and charge of keeping a registry or register and is charged with keeping authoritative and reliable records (*IPC Order 2001-029*).

A *registry* means a book authorized or recognized by law, kept for recording or registration of facts or documents (*IPC Order 2001-029*).

The Commissioner has considered the meaning of the term *office* in two Orders. In a decision relating to Vital Statistics Services (**section 4(1)(l)(vi)**), the Commissioner found that the term *office* was not limited a physical office but applied to the functions and duties associated with that office (*IPC Order 2001-014*).

Similarly, the office of the Registrar of Motor Vehicle Services (**section 4(1)(l)(ii)**) includes not only the Registrar's physical office, but also the information systems that pertain to the Registrar's official capacities (*IPC Order 2001-029*).

*IPC Order 2000-022* defined a *record made from information in a Land Titles Office* to mean a record made from information that related to the search, registration or filing functions of a land titles office.

To be excluded under **section 4(1)(l)(vii)**, two conditions must be present. The registry operated by a public body must be authorized or recognized by an enactment, and public access to the registry must normally be permitted (*IPC Order 2001-029*).

The exclusion in **section 4(1)(l)** applies to any record made from information in such a registry, whether the record is in the custody of the public body operating the registry or of another public body.

The exclusion does not apply if the requested information is not the same as what is publicly available from that Registry (see *IPC Order 2000-024*).

#### **Records of elected officials of local public bodies**

**Section 4(1)(m)** A personal or constituency record of an elected official of a local public body, such as a school trustee, a municipal councillor or a Metis settlement councillor, is excluded from the *FOIP Act* (see *IPC Order 99-032*). The onus will be on the elected official to show that the records are not related in any way to the business of the municipality, school board, Metis settlement, or other local public body to which the official has been elected.

*Personal records* are records that relate to an official as a private individual rather than as an elected official of the local public body.

Examples of personal records of an elected official that may be located on the premises of a local public body include

- private correspondence of an elected official that has not been sent or received by the official in his or her capacity as an officer of the local public body;
- records related to a community organization or non-profit group to which the official belongs on a personal basis and not as a representative of the public body;
- records related to a commercial or private business enterprise in which the official is employed, holds office or of which he or she is an owner, director, shareholder or partner; and
- records of personal or family appointments or events, such as medical appointments, birthdays, vacations and financial transactions.



*Constituency records* are records that relate to an elected official's constituency business, persons who may have worked on an election campaign and details about the campaign (*IPC Order F2005-010*). Examples of such records include:

- records relating to the election campaign of an elected official of a local public body, other than those records required to be submitted to the authority governing the election; and
- personal notes created solely as a memory aid and not scheduled for retention by the public body.

The following are useful guidelines for elected officials in determining whether a record is excluded from the scope of the Act:

- the record is not deposited with the administration of the local public body;
- the local public body has no power to compel the elected official to produce the records, even when referred to in a meeting of elected officials;
- the local public body has no authority to regulate or dispose of the records;
- the record exists and is referred to as a part of the elected official's mandate to represent the constituent, not as a basis for action by the local public body;
- the record is not integrated with other local public body records in the office of the elected official.

For more information on this exclusion, see FOIP Bulletin No. 6: *Records of Elected and Appointed Officials of Local Public Bodies*, published by Access and Privacy, Service Alberta.

***Personal records of appointed or elected members of the governing body of a local public body***

**Section 4(1)(n)** Personal records of appointed or elected members of governing bodies of local public bodies are excluded from the Act.

*Governing body* means the body that has the statutory authority to govern and make decisions affecting the local public body. This includes charter school boards, irrigation district boards and boards of housing management bodies. For universities, technical institutes, public colleges and the Banff Centre, the term is defined in **section 4(2)** to mean the board of governors and the general faculties council or academic council of the post-secondary body, as applicable.

In addition to the relevant examples cited above with respect to elected officials (**section 4(1)(m)**), the exclusion for personal records of appointed governing body members might cover

- records related to a professional or similar organization to which the individual belongs or in which he or she holds office;
- biographical and historical material about the individual which has not been made public;
- records related to previous jobs or appointments of the appointee;
- references given to individuals not employed by the local public body; or

- research, speeches, lecture notes and similar items which are not related to the local public body and which were not produced at the expense of the local public body.

The exclusion does not apply to personal information in records related to the mandate and functions of the governing body or related to the member in his or her capacity as an employee.

For more information on this exclusion, see FOIP Bulletin No. 6: *Records of Elected and Appointed Officials of Local Public Bodies*, published by Access and Privacy, Service Alberta.

***Personal or constituency records of a member of the Executive Council***

**Section 4(1)(o)** A personal record or constituency record of a member of the Executive Council is not within the scope of the Act. This means that records that relate to the duties of a member of the Executive Council as an MLA are excluded from the scope of the Act, but records that relate to duties in Cabinet and in the administration and operation of a public body are within the scope of the Act. Examples of constituency records and the guidelines for elected officials are discussed in relation to **section 4(1)(m)** earlier in this chapter.

***Records of the Speaker or an MLA that are in the custody or control of the Legislative Assembly Office***

**Section 4(1)(p)** A record created by or for the office of the Speaker of the Legislative Assembly or the office of a Member of the Legislative Assembly that is in the custody or under the control of the Legislative Assembly Office is not within the scope of the Act (see *IPC Order 97-017*).

*Created by or for* has been interpreted by the Commissioner to mean created by or on behalf of (*IPC Order 97-007*).

***Correspondence of Ministers, MLAs and agency heads***

**Section 4(1)(q)** This provision excludes certain records created by or for

- a member of the Executive Council;
- a Member of the Legislative Assembly; or
- a chair of a Provincial agency, as defined in the *Financial Administration Act*, who is a Member of the Legislative Assembly.

*Created by or for* means created by or on behalf of a Minister, MLA or agency head. In order to be excluded from the scope of the Act, the record must have emanated from the office of the Minister, MLA or agency head and must have been sent, or be intended to be sent, to one of the persons listed above (see *IPC Order 97-007*).

This exclusion does not generally apply to records created by officials or employees performing their duties under their governing legislation. It also does not apply to reports (e.g. an investigation report under section 15.1 of the *Social Care Facilities Review Committee Act* or an annual report) that a **Schedule 1** public body must provide to a Minister.

**Section 4(1)(q)** allows for the exclusion of certain records of Cabinet Policy Committees, where information that may eventually form part of the discussions of the Executive Council, the Treasury Board or one of their respective committees is exchanged and is the subject of discussion, consideration, advice and recommendation. The provision also excludes certain records of boards and agencies chaired by an MLA. Examples include the Seniors Advisory Council for Alberta and the Northern Alberta Development Council.

The exclusion extends to copies of such records sent to others, including officials in a public body (see *IPC Order 99-005*).

The exclusion applies to an attachment only if **section 4(1)(q)** applies individually to the attachment. The fact that a Minister attaches a covering letter to a record authored by someone else (and not emanating from the Minister's Office) does not mean that the Minister "created" the record (see *IPC Order 2000-013*).

If a record is created by a person who acts on behalf of one of the classes of persons listed in **section 4(1)(q)**, the exclusion applies only if the record indicates that the individual is acting on that person's behalf, or this is evident in some other way (see *IPC Order 96-020*).

#### **Alberta Treasury Branch records**

**Section 4(1)(r)** Records in the custody or under the control of an Alberta Treasury Branch, other than a record that relates to a non-arm's length transaction between the Government of Alberta and another party, are excluded from the coverage of the Act. The Act does not apply to the banking records of individuals, corporations and organizations that deal with the Alberta Treasury Branches.

In order for this exclusion to apply, the record must be in the custody of the Alberta Treasury Branch or under its control. The Treasury Branch must either have possession of the original record or some authority to manage it (see *IPC Order 98-019*).

A *non-arm's length transaction* is defined, for the purposes of this provision, and the following provision concerning credit union records, as any transaction that has been approved by

- the Executive Council or any of its committees;
- the Treasury Board or any of its committees; or
- a member of the Executive Council (**section 4(4)**).

This definition does not apply to **section 16** of the Act (see *IPC Order 98-013*).

#### **Credit union records**

**Section 4(1)(s)** The following records relating to credit unions are excluded from the Act:

- records relating to the business or affairs of Credit Union Central Alberta Limited, a credit union or a dissolved credit union; and
- records relating to an application for incorporation as a credit union.

In both cases, the records must be obtained or produced in the course of administering or enforcing the *Credit Union Act* or the regulations under it, and must relate to a transaction that is not a non-arm's length transaction as described above with respect to **section 4(1)(r)**. See *IPC Order 97-003* for a further discussion of credit union records.

***Credit union records respecting loans assumed by the Credit Union Deposit Guarantee Corporation***

**Section 4(1)(t)** The Act does not apply to a record of information referred to in section 120(3) of the *Credit Union Act* (advertising of long-term unclaimed balances) or respecting loans made by a credit union that are subsequently assumed by the Credit Union Deposit Guarantee Corporation.

***Health information of a public body that is a custodian under the Health Information Act***

**Section 4(1)(u)** This provision excludes health information, as defined in the *Health Information Act*, that is in the custody or under the control of a public body that is a custodian, as that term is defined in the *Health Information Act*.

If a public body that is a custodian under the *Health Information Act*, such as Alberta Health Services, receives a request for access to an individual's own personal information, the rules regarding access to information under the *Health Information Act* apply to the individual's health information, as defined in section 1(1)(k) of the *Health Information Act*. The rules regarding access to information under the *FOIP Act* apply to the individual's other personal information, as defined in **section 1(n)** of the *FOIP Act*.

**Records excluded from Part 1 only**

In addition to the exclusions in **section 4**, which remove the specified records from the scope of the FOIP Act, **section 6** of the Act contains two partial exclusions. An applicant cannot request access to these records, but other provisions of the Act apply to the information, including all the privacy protections.

***Briefing books***

**Section 6(4)** The right of access under the *FOIP Act* does not extend to a record created solely for the purpose of briefing a member of the Executive Council assuming responsibility for a ministry (**section 6(4)(a)**).

Within the Government of Alberta, when a new Minister assumes responsibility for a ministry, the Department normally prepares a briefing book for the Minister. This briefing material is compiled to allow the Minister to quickly gain an overview of the ministry's functions that will allow him or her to assume leadership of the ministry, to report on the ministry in Cabinet, and to represent its interests.

The briefing material will generally include some information that is publicly available, such as the ministry's business plan and annual report, as well as information created specifically for the new Minister, such as current assessments of operations and analysis of issues affecting the ministry. An applicant cannot request a

new Minister's briefing book for a period of five years from the date of the Minister's appointment as head of the ministry (**section 6(5)**).

Departments generally also prepare briefing binders for the Minister in preparation for a sitting of the Legislature. The purpose of the briefing material is to update the Minister on the status of ministry initiatives and to provide information in a convenient form. This enables the Minister to respond in a timely way to questions in the Legislative Assembly.

An applicant cannot request a Minister's briefing book for a sitting of the Legislative Assembly (**section 6(4)(b)**). This exclusion applies for a period of five years from the beginning of the sitting for which the record was created (**section 6(6)**).

A public body is not obliged to provide access to either of these kinds of briefing binders *in their entirety*, since the record *as a whole* was created solely for the purpose of briefing the Minister for one of the purposes specified in this exclusion.

These exclusions for briefing books do not apply to other kinds of briefing notes, including an item in one of the excluded briefing books that also exists in another file.

#### ***Records relating to an audit by the Chief Internal Auditor of Alberta***

**Section 6(7)** The role of the Chief Internal Auditor is to provide independent, objective assurance and advisory services to improve the effectiveness, efficiency and economy of government operations.

The exclusion in **section 6(7)** is a more limited version of the exclusion that applies to the Auditor General (**section 4(1)(d)**). The right of access to a record under the *FOIP Act* does not extend to a record relating to an audit by the Chief Internal Auditor of Alberta that is in the custody of the Chief Internal Auditor of Alberta or any person under his or her administration (e.g. an auditor employed under contract). The exclusion applies to records created by or on behalf of the Chief Internal Auditor as well as records supplied to the Chief Internal Auditor.

The exclusion under **section 6** does not apply

- if 15 years or more has elapsed since the audit to which the record relates was completed (**section 6(8)(a)**), or
- if the audit to which the record relates was discontinued or if no progress has been made on the audit for 15 years or more (**section 6(8)(b)**).

This exclusion does not apply to records relating to an audit by the Chief Internal Auditor that are in the custody of another public body. Those records are subject to **section 24(2.1)**, which is a mandatory exception to disclosure. For further information on **section 24(2.1)**, see section 4.10 in Chapter 4.



### Accounting for excluded records

Where excluded records or information form a portion of the records responsive to a FOIP request, a public body should consider whether the request for access to the information could be accommodated outside the FOIP process.



**Where the public body decides to disclose excluded records, the response to the applicant should explain that the records are excluded from the *FOIP Act*, and that the public body has decided to provide them outside the FOIP process in this case. Where an excluded record or part of a record forms a portion of the records responsive to a request and it will not be disclosed, the public body should indicate that the record, or part of the record, is excluded. (See Model Letter H in Appendix 3.)**

It is within the Commissioner's jurisdiction to determine whether an exclusion applies to a particular record or part of a record. The Commissioner has no jurisdiction over records that do not fall within the scope of the *FOIP Act* (see *IPC Order 99-034*).

If a public body applies an exclusion, it is not necessary to notify an applicant of all exceptions that the public body may claim if the Commissioner finds, on review, that the exclusion does not apply (see *IPC Order 99-033*).

If there is a request for review by the Commissioner, and the Commissioner finds that the information is not excluded, an opportunity will be given to the public body to consider any exceptions that may apply. See *IPC FOIP Practice Note 4: Section 4 – Exclusions from the Act*, published by the Office of the Information and Privacy Commissioner.

---

#### 1.6 Relationship to Other Acts

### Paramountcy

**Section 5** states that, if a provision of the *FOIP Act* is inconsistent or conflicts with another enactment, the provision of the *FOIP Act* prevails unless

- another Act; or
- a regulation under the *FOIP Act*

expressly provides that the other Act or regulation, or a provision of it, prevails over the *FOIP Act*.

A number of Alberta Acts contain paramountcy provisions that state that a provision of that Act prevails despite the *FOIP Act* (e.g. the *Municipal Government Act*, sections 299 to 301). (See the listing of the provisions of Acts and regulations that are paramount over the *FOIP Act* on the FOIP website: [foip.alberta.ca](http://foip.alberta.ca)). Other sections of Acts and regulations that prevail despite the *FOIP Act* are listed in **sections 15 and 17** of the FOIP Regulation.



**Section 5** of the FOIP Act provides the means for

- resolving an inconsistency or conflict between the *FOIP Act* and a provision of another Act or regulation, where neither the other Act nor the FOIP Regulation says that the other provision prevails despite the *FOIP Act*, or
- applying a provision in another Act or the FOIP Regulation that says that a provision of another Act or regulation prevails despite the *FOIP Act*.

When considering records that might be subject to a paramountcy provision in other legislation, a public body has to be sure that the record(s) being reviewed contain the kind of information that is referred to in the other Act or regulation. If the other Act or regulation refers to a certain category of information, such as a “report of a *Securities Act* investigator” or “adoption information” under the *Child, Youth and Family Enhancement Act*, the information requested must be able to be characterized in that way (see *IPC Order 99-027*).

The public body must then determine whether that other Act or the FOIP Regulation expressly states that the relevant provision of the other enactment prevails despite the *FOIP Act*. If so, this will mean that, in most cases, the public body will apply that other enactment on its own terms. For a more detailed discussion of how to apply paramountcy provisions, see FOIP Bulletin No. 11: *Paramountcy*, published by Access and Privacy, Service Alberta.

If the Information and Privacy Commissioner finds that a provision of an enactment prevails despite the *FOIP Act*, the Commissioner has no jurisdiction with respect to a matter that is subject to that provision (see *IPC Orders 99-034* and *F2005-007*).



**Public bodies considering making any provision of an Act or regulation paramount, in whole or in part, over the *FOIP Act*, must consult with Access and Privacy, Service Alberta, and with the Office of the Information and Privacy Commissioner during the consideration and drafting process.**

### Copyright Act

Section 32.1 of the *Copyright Act* (Canada) states that disclosure of a record pursuant to the *Access to Information Act* (Canada), or disclosure pursuant to any like Act of the legislature of a province, does not constitute an infringement of copyright. The *Copyright Act* may apply to the subsequent use or disclosure of that record by the recipient.

Public bodies are not infringing copyright by disclosing copyright material in response to a FOIP request. However, it may be relevant to consider the application of **section 29** of the *FOIP Act* (information that is or will be available for purchase by the public).







## 2. ADMINISTRATION OF THE FOIP ACT

### Overview

This chapter covers

- the roles and responsibilities of various public body officials;
- the delegation of FOIP responsibilities;
- the roles of the Information and Privacy Commissioner, the Minister responsible for the *FOIP Act*, and Access and Privacy, Service Alberta;
- practices of routine disclosure and active dissemination;
- the exercise of individual rights by authorized representatives;
- notices and the manner of giving notice;
- the directory of public bodies and personal information banks;
- accessing manuals and guidelines;
- the protection from liability for public bodies and their officials;
- offences and penalties; and
- disclosure to the Commissioner.

### 2.1

#### Public Body – Roles and Responsibilities

#### Head of a public body

The head of each public body is responsible for all decisions made under the *FOIP Act* that relate to that public body. If the public body is a department, branch or office of the Government of Alberta, the head is the member of the Executive Council (the Minister) who presides over the public body (**section 1(f)(ii)**).

For other public bodies that are not local public bodies (i.e. agencies, boards, commissions, etc. designated in the FOIP Regulation), the head is the person designated by the member of the Executive Council responsible for that public body. If a head is not so designated, the person who acts as the chief officer and is charged with the administration of the body is the head (**section 1(f)(ii)**).

The provision for designation of a head by a Minister recognizes that small government agencies may receive support services from a government department. In these cases, the member of Executive Council responsible for the agency can assist them by designating a head for the purposes of the *FOIP Act*, for example, a person from within the department.

For local public bodies, the head is the person or group of persons designated by bylaw or other legal instrument to perform the duties of the head for purposes of the Act (**sections 1(f)(iii) and 95(a)**).

In any other case, the head is the chief officer of the public body (**section 1(f)(iv)**).

The governing authority of a local public body will normally designate its chief administrative officer, or equivalent, as head. Examples include a president of a

post-secondary educational institution, a city or town manager, a head librarian, and a school superintendent. However, the governing authority may decide to appoint a committee to fulfil this role.



**Governing authorities of local public bodies must designate a head by bylaw or by another legal instrument by which they act.**

### **FOIP Coordinator**

The Minister responsible for the *FOIP Act* and Regulation requires that each public body establish an office or function that is responsible for FOIP matters and have a key contact person who can carry out this function.

The function is usually performed by a FOIP Coordinator. The FOIP Coordinator is responsible for the overall management of access to information and protection of personal information within a public body. Depending on the size and resources of the public body, the FOIP Coordinator may carry out his or her responsibilities on a full-time or part-time basis, or may be someone appointed from outside the public body to carry out FOIP responsibilities on its behalf. Some FOIP Coordinators provide shared services for several public bodies.

The FOIP Coordinator's office should provide the focal point for access to information and protection of privacy expertise within the public body. Details of the responsibilities of this office throughout this publication represent a typical distribution of responsibilities for a FOIP Coordinator. Public bodies may find that a different distribution of responsibilities is appropriate for them.

The responsibilities include

- implementing policies, guidelines and procedures to manage the public body's compliance with the Act;
- ensuring that the public body has a delegation instrument in place and that public body staff understand their roles under the Act;
- providing advisory services to the staff of the public body;
- providing training programs on access to information and privacy protection within the public body and coordinating participation in FOIP courses offered by the Government of Alberta;
- informing the public body's clients, and all those with which it does business or provides services, about the Act;
- advising senior management on information that can be disclosed without a FOIP request;
- managing the FOIP request process for the public body, which may include
  - assisting applicants;
  - assigning requests to program areas;
  - monitoring and tracking the processing of requests;
  - meeting time limits and notification requirements;



- considering representations from third parties;
- calculating fee estimates and collecting fees;
- reviewing preliminary recommendations from program areas and offices of the public body about the disclosure of records and proposals for severing information;
- making final recommendations on responses to requests; and
- responding to applicants;
- coordinating any negotiations, mediations, inquiries, investigations, and audits with the Office of the Information and Privacy Commissioner;
- setting up practices and procedures to ensure compliance with the privacy protection measures in **Part 2** of the Act regarding the collection, use, disclosure, accuracy, retention and security of personal information;
- ensuring that the public body staff are aware of other Acts and regulations that restrict the disclosure of information (**section 5**) so that the provisions of such Acts and regulations are applied consistently;
- reporting as required to the Ministry responsible for the *FOIP Act* on the operation of the Act; and
- maintaining and publishing a Directory of Personal Information Banks and coordinating the public body's submission to the Directory of Public Bodies published by the Minister responsible for the *FOIP Act*.

In the case of public bodies that have affiliated agencies, boards and commissions, responsibilities also include

- maintaining a list of the public body's affiliated agencies, boards and commissions for the purposes of **Schedule 1** of the FOIP Regulation; and
- consulting with Access and Privacy, Service Alberta, regarding any legislative developments or amendments in other legislation that might relate to the *FOIP Act*.

### **Program administrators**

In larger or decentralized public bodies, program administrators or department heads have special responsibilities for ensuring effective administration of the *FOIP Act*.

Normally, they are accountable for

- setting up practices and procedures to ensure that the management and security of records in the custody or under the control of their program area meet the requirements of the legislation, especially the provisions relating to the protection of privacy;
- identifying and providing access to information that can be disclosed without a FOIP request;
- locating and retrieving records in response to FOIP requests; and
- ensuring that the program perspective is considered in any recommendation on a response to a FOIP request.

Where the administration of the *FOIP Act* is decentralized, each program should have an appointed program contact to ensure that requests are processed effectively, that information that can be routinely disclosed is identified, and that privacy protection measures are implemented.

### **Public relations or communications**

In public bodies with a public relations or communications area, staff in that area may have a direct role in the access to information and protection of privacy function. Disclosure of information in response to access requests under the *FOIP Act* should be coordinated with the overall flow of information to the public where possible. Where a public body is providing information on sensitive issues, either on its own initiative or in response to a FOIP request, the public body may find it helpful to have a communications strategy for disclosure of the information. At the same time, communications staff must bear in mind that the *FOIP Act* determines what may or must be disclosed in response to a request under the Act and establishes time limits for disclosing records in response to a request.

Routine disclosure of information in response to a routine inquiry or request, active dissemination of information, and publication of information in print and electronic formats should continue to be the normal ways of serving those interested in obtaining information.

### **Records and information management**

Effective records and information management within a public body plays a major part in the effective administration of the *FOIP Act*. The same is true of the information technology function relating to the management of electronic information systems, databases and other electronic records.



Each public body should coordinate its efforts for managing, administering, controlling, providing security for, and preserving all its records. Records include electronic data and information, publications and other reports in the custody or under the control of the public body. These efforts will ensure that the public body can meet its requirements under the Act.

Records and information management and information technology professionals can provide support to the FOIP Coordinator by

- establishing and maintaining an adequate level of information control to ensure that all records can be located and retrieved within the required time limits;
- establishing and maintaining information management systems for the public body that comply with the Act's privacy protection provisions;
- creating a listing of all personal information banks;
- ensuring that records retention and disposition schedules are established, authorized as required, and applied to all information in the custody or under the control of a public body; and

- providing a basis for implementing information security measures for sensitive records and for the reasonable protection of personal information.

Additional guidance on records and information management practices is provided in Chapter 8.

## 2.2 Delegation of FOIP Responsibilities

Under 85 of the Act, the head of a public body has the power to delegate to any other person any of the head's duties, powers and functions under the Act, except the power to delegate.

In a very small public body, where the designated head may also be the FOIP Coordinator, there will generally be no need to delegate. In larger public bodies, a delegation instrument will be needed. The FOIP Coordinator normally prepares the delegation instrument and submits it to the head of the public body for approval.



All public bodies that decide to delegate some or all of the head's powers and duties should have an up-to-date delegation instrument in place. This means that the delegation instrument should be reviewed regularly for any necessary changes related to restructuring of the public body. It should also be reviewed with a new head to confirm that the head agrees with the scheme of delegated responsibilities.

The delegation instrument should identify the position, not the individual, to which the powers are delegated. When delegation is to the position rather than the person, a new delegation is not required when a new appointee assumes the position or when someone is acting in the position. A delegation instrument may also recognize another position to which delegation passes if the occupant of the original position is absent or incapacitated. A delegation instrument may cover a wide variety of duties, powers and functions, including those under the *FOIP Act* as well as others.

A delegation instrument remains in effect until replaced. It is important to review the instrument periodically for any changes that may be needed, especially if the public body is restructured or part of the public body is transferred to another public body.

There is a substantial difference between delegations relating to access to information and those relating to protection of privacy. In the case of access to information, the delegations relate mostly to the processing of an access request and the decision whether or not to disclose all or part of a record. Delegated authority empowers certain officials and employees to make decisions or take action. In the case of privacy protection, responsibilities centre on the collection, handling and protection of personal information. This is a much more general area of responsibility and is centred on the program areas or local offices that handle the information on a day-to-day basis. Even in small public bodies, most privacy protection responsibilities should be delegated to staff in the program areas responsible for the information.

Not every section of the Act dealing with privacy matters calls for delegation of responsibility in a formal sense. The head of a public body should, however, clearly

advise program administrators and managers of their responsibilities, especially with regard to compliance in the collection and disclosure of personal information.

In general, delegation should be considered for all provisions of the Act that state that the head of a public body may or must do something. A **Delegation Table** that lists all the provisions of the *FOIP Act* for which delegation should be considered is provided in Appendix 2.1. A table listing all the administrative responsibilities that may be assigned (particularly those under **Part 2** of the Act) is provided in Appendix 2.2. Public bodies need to customize these listings to their actual operations. This includes using the organization's own position titles and providing for delegation to positions in multiple departments, branches or offices where appropriate (e.g. delegation of powers and duties relating to different regions to the director of each regional office of the public body).

The **Delegation Table** provides for the identification of specific officials by title and office (e.g. the Executive Manager, Personnel) and for generic titles such as "all program managers (for their respective program areas)."



It is essential when a delegation instrument is put in place that all identified officers or employees know and understand their delegated responsibilities. It is also important for other officers and employees to understand that only those with delegated responsibilities under the *FOIP Act* should be carrying out those duties or functions.

For example, a public body's lawyer is not authorized to respond to an access request unless the head has delegated that authority to the lawyer under **section 85** (see *IPC Investigation Report 99-IR-009*).

At the same time, a public body official may sign a document advising an applicant of a decision under the *FOIP Act* on behalf of the person who has been delegated to make the decision, provided it is clear that the delegate has directed his or her mind to the making of the decision. This may be the case if the head of the public body has retained the power to make a particular decision, but the FOIP Coordinator is generally responsible for corresponding with the applicant.

For example, in *IPC Investigation Report 98-IR-011*, it was reported that the Minister of Justice and Attorney General had delegated to the Chief of Police of a police service the authority to disclose information about an individual believed to present a risk of significant harm to the health or safety of persons in that community, in accordance with an approved disclosure protocol. Although the Chief of Police (the delegate) made the decision regarding the disclosure, the information was disclosed through a news release issued by the police service. The Information and Privacy Commissioner determined that the disclosure was in accordance with the *FOIP Act*.

Job orientation materials for employees should include a statement about FOIP responsibilities for each official or employee taking up a position that includes delegated responsibilities under the Act. The employee should also be advised that additional information can be obtained from the FOIP Coordinator.

The way in which powers and duties are delegated in practice is very much determined by the structure of the public body and the approach that it wishes to take toward administration of the *FOIP Act*. Delegation is decided in consultation with elected officials or governing board members and senior management in the public body. In smaller public bodies, for instance, the head may choose to delegate to a single official. In larger public bodies or in decentralized organizations, the head may wish to spread decision-making responsibilities more widely, to department heads or other staff.

If the individual with delegated authority does not actually make the decision that he or she has been authorized to make, the delegation has not been properly exercised. Once a delegate makes a valid determination or decision in the proper exercise of the delegated power, the head of the public body cannot redetermine the matter or substitute his or her decision for that of the delegate.

It is also important not to fetter or restrict the discretion of a delegate. In *IPC Investigation Report 98-IR-011*, the Commissioner considered it important that the Disclosure Protocol for Chiefs of Police that he reviewed as part of the investigation did not fetter the discretion of the Chief to decide whether to disclose personal information about an individual and how much or what personal information to disclose about the individual.

### 2.3

#### Province-wide Administration of the Act

#### Minister responsible for the *FOIP Act*

The Lieutenant Governor in Council designates the Minister responsible for the Act by Order in Council. In March 2008, the Minister of Service Alberta was given this responsibility. The Minister has overall responsibility for the general administration of the Act across the province, including preparation and submission of amendments to the *FOIP Act* and FOIP Regulation and providing guidance about access to information and protection of the privacy of personal information generally.

The Minister is required to report annually to the Legislative Assembly on the administration of the Act (**section 86**). The Minister is also responsible for publishing a Directory of Public Bodies, including the names of all public bodies, and business contact information for their FOIP Coordinators or heads (**section 87**).

#### Access and Privacy, Service Alberta

Access and Privacy supports the Minister responsible for the *FOIP Act* and Regulation in all aspects of the administration of the legislation across all public bodies. Access and Privacy provides public bodies with the following services and products related to the FOIP program:

- the development of proposals for amendments to the *FOIP Act* and the FOIP Regulation, as well as the development of Ministerial Regulations for the designation of public bodies in between updates to the Schedule of public bodies in the FOIP Regulation;
- the development of guidelines and best practices, where appropriate or needed, to assist public bodies in administering the legislation;



- the production of resources to enable FOIP Coordinators and others in public bodies to remain up-to-date on issues and trends in the fields of access to information and the protection of privacy;
- guidance on the interpretation of the Act and Regulation, including a “help desk” to assist public bodies;
- regular distribution of updated FOIP legislation and policies, as well as access to Orders and Investigation Reports issued by the Information and Privacy Commissioner and other related information;
- delivery of regular FOIP training sessions and seminars;
- an electronic tracking system for FOIP requests and statistical reporting which may be used by public bodies; and
- collection of statistical information for the Annual Report and contact information for the Directory of Public Bodies.

### **Key departments**

There are a number of departments that have statutory responsibilities relating to particular local public bodies. These include the provincial ministries of Municipal Affairs, Education, Advanced Education, Health and Wellness, Solicitor General and Public Security, Aboriginal Relations, Culture and Community Spirit, Environment, and Agriculture and Rural Development.

Key departments assist local public bodies in resolving administration and compliance issues relating to the Act. Key departments are also partners with Access and Privacy in answering questions, resolving issues, sponsoring meetings and other training forums, and providing speakers in the area of access to information and protection of privacy.

### **Information and Privacy Commissioner**

The Information and Privacy Commissioner is an officer of the Legislature who is independent of government. The Commissioner is responsible for monitoring how the legislation is administered to ensure that its purposes are achieved. He or she may carry out investigations to ensure compliance with any provision of the Act or compliance with rules relating to the destruction of records. The Commissioner may be asked to provide an independent review of decisions made under the Act. He or she may make an order regarding duties imposed by the Act (e.g. ordering the disclosure of certain records), administrative matters (e.g. reducing a fee assessment) and the collection, use or disclosure of personal information.

The Commissioner reports annually to the Speaker of the Legislative Assembly on the operation of the legislation (**section 63**). The powers of the Commissioner and the role of the Office of the Commissioner are discussed in Chapter 10.



## 2.4

### Routine Disclosure and Active Dissemination of Information

In addition to providing access to records and information in response to FOIP requests under **Part 1** of the Act (see Chapter 3), public bodies may provide access to information and records through two other processes:

- routine disclosure in response to inquiries and requests for information; and
- active dissemination of information.

Routine disclosure and active dissemination will likely satisfy many of the information needs of members of the public. Public bodies should bear in mind that the FOIP process is in addition to and does not replace existing procedures for access to information (**section 3(a)**), where that disclosure would not otherwise be prohibited by the *FOIP Act*.

There are numerous advantages to using routine disclosure and active dissemination processes. The public will be better served and better informed through the planned and targeted release of information in support of overall program objectives. As well, making information available outside the FOIP process, through disclosure in response to routine inquiries and requests or active dissemination of information, can promote cost-effective management of public information resources.

#### Routine disclosure

The *FOIP Act* is intended to strengthen informal access rights by encouraging routine disclosure and requiring public bodies to provide access to decision-making manuals (**section 89(1)**). (See section 2.8 of this chapter for further discussion of what is meant by decision-making manuals.)

*Routine disclosure*, in response to an inquiry or request, occurs when access to a record can be granted without a request under the *FOIP Act*.

For example, a public body may have a routine disclosure policy regarding information related to an appeal process, such that an appellant does not need to make a FOIP request to obtain that information. In a case involving this kind of information, the Information and Privacy Commissioner found that the public body had properly responded to a request from an appellant for information related to an appeal when it disclosed information in accordance with the public body's routine disclosure policy and not under the *FOIP Act* (*IPC Order 2001-013*).

If a request cannot be satisfied entirely through routine disclosure, then the request may be dealt with in part through routine disclosure and in part through the FOIP request process. For example, a public body might provide the final report of an administrative review through a process of routine disclosure, but would not routinely disclose research for the report and preliminary drafts of the report.

If there are two processes for obtaining access to information, such that a public body will provide routine disclosure to an individual of information in his or her own file in addition to providing access in response to a FOIP request, then the public body should advise individuals of the two processes. Public bodies should ensure that individuals are aware of both their statutory rights under the Act and the availability of any other method of access.

Where two processes exist, a public body meets its duty to assist an applicant under **section 10(1)** only if it informs the applicant that the two processes are in place (see *IPC Order 98-002*).

**Section 88(2)** enables a public body to set fees for the provision of information through routine disclosure, unless records can otherwise be accessed without a fee.

Public bodies may consider the appropriateness of routine disclosure in the following situations:

- disclosure is required or permitted by another federal or provincial statute or regulation or by a municipal bylaw;
- **section 40** of the *FOIP Act* permits disclosure and any conditions specified in **section 40** apply in the circumstances;
- no exceptions to access would apply if the records were requested under the *FOIP Act*;
- any exceptions that apply to a class of records are not mandatory exceptions, and the public body, if it received a request for the particular class of records, would not invoke any discretionary exceptions to refuse access; or
- an exception does apply to a class of records, but the information subject to the exception can easily be severed from the other information and that other information may be routinely disclosed.

There are several ways in which public bodies may make information accessible through routine disclosure.

### ***Answers to particular questions***

Public bodies handle a large number of inquiries from members of the public seeking the answer to a question rather than asking for access to records. Occasionally, a person will combine a question with a request for records. To the greatest extent possible, public bodies should deal with these questions without a FOIP request through information offices or the appropriate program area and approval process.

If it becomes clear that the request involves records that cannot be routinely disclosed, such as personal information about a third party, the person making the request should be referred to the FOIP Coordinator's office. That office could either advise the applicant to make a FOIP request under the Act or give advice to the program area on how the records should be severed before being disclosed.

### ***Specifying categories of records for routine disclosure***

**Section 88(1)** of the Act provides that public bodies may specify categories of records in their custody or under their control that will be made available to the public without a request for access under the Act. In this way, public bodies can take a proactive approach by setting up channels for the release of information and identifying records that are available without a FOIP request. This approach promotes openness and accountability in a public body.

**Active dissemination**

*Active dissemination* occurs when information or records are periodically released, without any request, under a program or communications plan.

Active dissemination is best used where there is an anticipated demand for information by the public. Active dissemination projects generally involve some investment by public bodies, and these costs have to be balanced against improved services to the public.

Active dissemination can take many forms. A public body may have an information centre where information can rapidly be gathered and sent to clients, by mail, fax or through electronic networks. Information may also be made available in a library or public reading area.

Public bodies can establish Internet sites or online databases where interested citizens can obtain information either through an intermediary or by direct online access. Reference databases may be used to answer queries from clients or made directly accessible online. Databases may also be distributed to libraries and other public facilities; private sector information services may be also used to make popular government or local public body databases available.

Much information is available in reports and publications through public body websites and through various program information offices. These may be made available either free of charge or for a price. To assist their staff and members of the public to access published materials, public bodies may wish to maintain listings of these materials through their communications office, library, information resource centre or the office of the FOIP Coordinator.

In deciding upon the method of active dissemination, public bodies should consider the accessibility of the information to the intended target audience. For example, a document that is intended to provide information to persons who may be visually impaired may not reach that audience if it is only made available in a small-print format.

**Practices for routine disclosure and active dissemination**

The following practices will support routine disclosure and active dissemination of information.

***Review information holdings***

In establishing a system of routine disclosure and active dissemination, public bodies should review their record holdings to determine where the practices may best apply.

Every jurisdiction that has implemented freedom of information legislation has found that there has been considerable ongoing demand for contracts, travel claims, major reports and plans, internal audits, tax and regulatory rulings, decisions of adjudicative tribunals, and inspection records, among other types of information.

In some instances, records may have to be written and prepared in a different way to facilitate access. For example, reports might be written in a more structured way, such that recommendations or personal information can easily be severed and the

remainder of the record made public. Where this is necessary, the public body should establish standards for the creation of these types of documents and ensure that its staff are familiar with them.

### ***Establish a coordinating committee***

Where a public body is large or decentralized, it may be advantageous to develop a network of contacts in program and administrative areas or in the public body's various locations or facilities. This may be built into a coordinating group that could, in consultation with the FOIP Coordinator, develop and help implement routine disclosure and active dissemination practices. The practices must be guided by and not contravene the *FOIP Act*. Members of such a group might include

- interested individuals from program areas with records that may qualify for routine disclosure and active dissemination;
- a communications officer who understands the information needs of clients and the general public;
- a representative of the records and information management practice area in the public body who has a good grasp of the types of records held by the public body;
- a representative from the information technology area who understands how the public body can use information networks to disseminate information;
- a FOIP Coordinator who understands how routine disclosure and active dissemination can assist the public body in dealing with the requirements of the *FOIP Act*; and
- a representative from the legal or legislative services area who understands the obligations of the public body under other legislation that may affect the kind of information that can be disclosed.

### ***Review requests for information***

The FOIP Coordinator or the committee should review the types of requests for information currently made to the public body to determine whether these can be met through either routine disclosure or active dissemination. The objective should be to respond to as many requests as possible outside the *FOIP Act*. This should involve an ongoing monitoring and review of FOIP requests to determine whether there are certain categories of requests that can be handled through routine disclosure.

### ***Delegate authority***

The public body may delegate authority for routine disclosure, under an appropriate delegation instrument, to the program area where the information is collected, compiled or created. The program area should, in accordance with the practices of the public body on routine disclosure, establish mechanisms for the rapid and effective release of the information. For further information on delegation, see section 2.2 of this chapter and Appendix 2.

In the case of active dissemination, an official in the program area may be delegated the responsibility for establishing a dissemination mechanism. The FOIP Coordinator should play an advisory role in establishing such mechanisms, monitoring what action has been taken, and obtaining information on how these mechanisms are working. A listing of records subject to routine disclosure and active dissemination

should be available to employees of the public body. Employees should receive training on assisting the public when a request is made for a record that falls within these categories and about referring members of the public to the appropriate office when it is not clear whether the information may be disclosed.

### **Create new records**

The FOIP Coordinator should be consulted when there are plans to create new types of records within the public body. This consultation will determine whether any of these new records could be made available through routine disclosure or active dissemination.

Consideration should be given, where possible, to modifying standard records by removing segments that would be subject to mandatory exceptions. For example, if a record contains both general information and personal information, but the main purpose of the record is to provide general information, then practices can be put in place to move personal information on to a separate page or suppress the fields for personal information in an electronic record. This may make the record available for either routine disclosure or active dissemination.

### **Special conditions for personal information**

Personal information requires special consideration when making decisions about routine disclosure.

Public bodies may be able to identify categories of records containing personal information that may be made available without an access request

- to the individual the information is about, or to the individual's personal representative (**section (84(1))**); or
- under the public body's governing legislation.

The public body must, when routinely disclosing personal information to the individual the information is about or under an enactment that authorizes disclosure to specific persons,

- verify the identity of the person to whom the information is disclosed; and
- ensure that any person exercising the rights of an individual under **section 84** of the Act provides appropriate written evidence of his or her right to exercise that individual's rights under the Act.

Designation of categories of personal information for routine disclosure to the individual the information is about is appropriate where a considerable demand occurs for a particular type of record. Making the process more routine, with fewer processes and approval requirements, can save a public body considerable time, effort and resources. An example of this process is providing a client with routine access to his or her file or an employee with routine access to his or her personnel records.





**When providing routine disclosure of information in an individual's own file, public bodies must ensure that disclosure of personal information of other individuals does not occur. Advice from the FOIP Coordinator should be sought on procedures for providing routine disclosure of these records.**

## **2.5 Exercise of Individual Rights by Authorized Representatives**

**Section 84** of the Act provides that another person, under specific circumstances, may exercise any right or power under the Act that is conferred on an individual. The specific circumstances in which a person may act for another individual, and the limitations that apply in each case, are discussed in this section.

### ***Deceased individual***

**Section 84(1)(a)** If an individual is deceased, the individual's personal representative (an executor under a will or an administrator under Letters of Administration) can exercise rights and powers under the Act. This exercise of rights and powers is limited to information relating to the administration of the individual's estate.

Proof of the right to act is normally a copy of the signed and attested document naming the representative to act in matters related to the estate. Evidence consisting of an applicant's stated belief in his or her authority, whether by affidavit or otherwise, or evidence that an applicant administered an estate is not sufficient (see *IPC Order 98-004*). For information related to disclosure to relatives of deceased persons, see section 4.3 in Chapter 4, and section 7.7 in Chapter 7. For a detailed discussion of information rights relative to deceased individuals, see also FOIP Bulletin No. 16: *Personal Information of Deceased Persons*.

### ***Guardian or trustee***

**Section 84(1)(b)** If a guardian or trustee has been appointed for the individual under the *Dependent Adults Act*, the exercise of rights can be undertaken only by the guardian or trustee. The rights or powers must relate to the powers and duties of the guardian or trustee. When the *Adult Guardianship and Trusteeship Act* is proclaimed in force, and repeals the *Dependent Adults Act*, there will be a broader range of roles to support adults with impaired capacity to make decisions. These new roles include co-decision-makers, specific and emergency decision-makers, as well as both temporary and permanent guardians and trustees. There will also be a registry to track court orders respecting guardianship and trusteeship.

The document governing the nature of the guardianship or trusteeship provides the authority for the representative to act. Public bodies should examine that document to ensure that the right being exercised under the *FOIP Act* is within the scope of the powers and duties set out in the guardianship or trusteeship document.

### ***Personal directive***

**Section 84(1)(c)** If an agent has been designated under the *Personal Directives Act*, the agent can exercise the individual's rights. The exercise of rights is limited to the powers and duties given to the agent under the personal directive. Personal directives cannot provide authority over financial matters.



Before allowing an agent to exercise the rights of the maker of a personal directive, a public body should satisfy itself as to the identity of a person who wishes to exercise the rights of an agent, and the authority of the person to exercise the rights of the maker of the personal directive. This may require examination of the personal directive and any necessary supporting documentation (such as a record of the determination of lack of capacity). Since this information is sensitive personal information of the maker of the directive, a public body should record only what is necessary to document the agent's authority to exercise the rights of the maker under the *FOIP Act*.

The *Personal Directives Act* provides for a registry of personal directives and permits the Minister responsible for that Act to disclose information in the Registry if, in the opinion of the Minister, the disclosure is in the best interest of the maker. The Act, as amended in 2008, also makes directives made outside Alberta valid when they consistent with Alberta's *Personal Directives Act*.

Further information about personal directives is available from the Office of the Public Guardian and online at [www.seniors.gov.ab.ca/opg/PersonalDirectives/](http://www.seniors.gov.ab.ca/opg/PersonalDirectives/).

### **Power of attorney**

**Section 84(1)(d)** A power of attorney is an authority given to one person (called the attorney) to do certain acts in the name of, and personally representing, the person granting the power (called the donor).

A power of attorney can be to perform specific acts on behalf of the donor or can be a general power of attorney to do everything that the donor can do. Some powers of attorney can be revoked by the donor; some are irrevocable. Powers of attorney come into effect in the event of mental incapacity or remain in effect notwithstanding the mental incapacity of the donor, provided they comply with the provisions of the *Powers of Attorney Act*. The death of a donor normally revokes the power of attorney.

A public body should satisfy itself that the scope of a power of attorney is sufficient to authorize the attorney to exercise the donor's rights under the *FOIP Act*. The public body should also verify the identity of a person exercising the power of attorney. It may also be necessary, depending on the nature of the power of attorney, to verify that the donor is alive.

### **Minors**

**Section 84(1)(e)** A guardian of a minor may exercise any right or power under the Act if the exercise of that right would not be an unreasonable invasion of the minor's privacy. For a public body to make that decision, the first step is to determine whether the person asserting guardianship is a legal guardian. The Information and Privacy Commissioner has said that it is the responsibility of the person asserting the right to exercise the rights of a minor to prove that he or she is the child's guardian (*IPC Order F2006-003*). The second step is to determine whether the exercise of the right or power by the guardian would be an unreasonable invasion of the personal privacy of the minor.

Guardianship is determined under two Acts. The federal *Divorce Act* applies to custody, access and child support matters in divorce proceedings. Alberta's *Family Law Act* defines legal parentage and provides for guardianship and parenting orders.

The *Divorce Act* does not use the term "guardian." The language of the *Divorce Act* focuses on "custody" and "access." If a spouse is granted custody of a child, he or she is entitled to make decisions regarding the care and control of the child.

The *Family Law Act* does not explicitly define "guardian," but indicates that, in most cases, parents are automatically the guardians of their children. Guardians are responsible for raising the child, providing day-to-day care, and supporting and nurturing the child's development.

The *Family Law Act* provides for the courts to make a "parenting order" if guardians are unable to agree on how to distribute the powers, responsibilities and entitlements of guardianship. Parenting orders may allocate powers among parents and limit the involvement of a parent.

Every child under the age of 18, except if married or in an adult interdependent relationship, is subject to guardianship. Parents are normally the guardians. Each guardian may exercise all the powers independently of the other, unless there is an agreement or court order to the contrary.

A public body that receives a request to exercise the rights of a minor under the *FOIP Act* will need evidence that an individual is authorized to exercise those rights. An individual could provide

- a custody order under the *Divorce Act*,
- a parenting order under the *Family Law Act*, or
- other evidence that would be considered reliable and appropriate in the circumstances (e.g. a statutory declaration may suffice in some cases).

A non-custodial parent with rights of access to the minor may have some limited rights to access information about his or her child (e.g. under the Student Record Regulation pursuant to the *School Act*) even if he or she is not the child's guardian.

Regardless of what evidence is provided in support of guardianship, the public body should verify the individual's identity (e.g. ask to see some form of valid photo identification, such as a driver's licence).

A public body that has determined that an individual is entitled to exercise the rights of a guardian must then consider whether it is appropriate in the circumstances.

**Section 84(1)(e)** is discretionary, and disclosure of the minor's personal information may be limited to circumstances where, in the opinion of the head of the public body concerned, the exercise of the right or power by the guardian would not constitute an unreasonable invasion of the personal privacy of the minor. Special care is required when the exercise of the rights of a minor relates to sensitive personal information of the minor.

When determining whether a minor can give a direction or make a decision that the public body may act upon, a public body should take into consideration its own

policies and procedures for assessing when a minor has the ability to understand the matter being decided and to appreciate the consequences of such a decision. The opinions and views of the minor must be taken into account in making this determination, except in cases where the minor is clearly too young or immature.

#### **Written authorization**

**Section 84(1)(f)** A written authorization is a document in writing signed by an individual who authorizes another individual to do certain acts in the name of and on behalf of the individual signing the document.

A written authorization should be to perform specific acts (e.g. provide consent, make a FOIP request on behalf of the authorizing individual) or, more generally, to exercise the rights or powers of the individual under the *FOIP Act*. Before disclosing personal information on the basis of **section 84(1)(f)**, public bodies may, in some circumstances, wish to contact the individual who has granted the authority to confirm that he or she is aware of the amount and type of personal information that will be disclosed. However, a public body cannot refuse to allow a person with a valid authorization to exercise the rights of an individual.

An example of an **Authorization of Representative Form** is included in Appendix 5.

## 2.6 Notice and Manner of Giving Notice

The Act contains requirements for giving various types of notices to persons. **Section 17(2)(b)** provides for a notice to be given to a third party when the third party's personal information is being disclosed for compelling health or safety reasons. **Sections 30 and 31** deal with notices to be given to third parties and to applicants during the access request process. **Section 32(4)** provides for notices to be given to a third party and to the Information and Privacy Commissioner when personal or confidential business information of a third party is being disclosed in the public interest. In addition, **section 80** provides for the Commissioner to notify parties respecting a review. The **Model Letters** in Appendix 3 provide examples and options for the notices that a public body may be required to give under the Act.

**Section 83** **Section 83** requires that any notice or document to be given to a person under the Act be given

- by sending it to that person by prepaid mail to the last known address of that person;
- by personal service;
- by substitutional service if so authorized by the Commissioner;
- by facsimile telecommunication; or
- in electronic form other than facsimile telecommunication if the person to whom the notice or document is to be given has consented to accept the notice or document in that form.

*Personal service* means a method of delivery whereby it can be shown that the person to be served actually received the document.

*Substitutional service* means the placing of public notices in a trade journal or in other specialized or general media. This method of service may be appropriate in situations where a very large number of persons need to be given notice or where a third party or other notice recipient cannot be located and the nature of the information would lend itself to this type of public notice.



Substitutional service can be used only with the permission of the Commissioner.

*Service in electronic form* means delivery in digital form or in any other intangible form by electronic, magnetic or optical means or by any other means with similar capabilities for creation, recording, transmission or storage. Whether a person has consented to accepting a notice in electronic form (e.g. by e-mail) is determined in accordance with section 8(2) of the *Electronic Transactions Act*. Under that provision, consent may be inferred from a person's conduct if there are reasonable grounds to believe that the consent is genuine and relevant to the information.

The provision allowing electronic transmission does not limit a public body's obligations under the Act with respect to personal privacy, rights of access to information and the protection of confidential information (section 3 of the *Electronic Transactions Act*). A public body must comply with the *FOIP Act*'s requirements for protection of personal information (**section 38**), making reasonable security arrangements to prevent unauthorized access. A public body must not disclose confidential business information in the course of the third party notice process by transmitting the information in an insecure manner. Also, a public body must not impair rights of access by limiting the manner in which a person can obtain access to information.

### Third party notices

When the head of a public body is considering giving access to a record that may contain information that affects the interests of a third party under **section 16** or the disclosure of which may be an unreasonable invasion of a third party's personal privacy under **section 17**, the head must give written notice to the third party and to the applicant in accordance with **sections 30 and 31** of the Act.

Public bodies should choose a delivery method that ensures that the notice arrives quickly and conveniently for a third party or other person receiving notice but also one that is efficient and cost-effective. Prompt delivery will allow the third party as much time as possible to respond. See Chapter 5 and FOIP Bulletin No. 10: *Third Party Notice*, published by Access and Privacy, Service Alberta.

**Section 84(2)** Any notice required to be given to an individual under the Act may be given to the person entitled to exercise the individual's rights and powers as provided for in **section 84(1)**.

## 2.7

## Directories

**Directory of public bodies**

**Section 87(1)** sets out the requirements for the Directory of Public Bodies that must be published by the Minister responsible for the Act. The directory must include the name of the public body and business contact information for the FOIP Coordinator or, if the public body has no FOIP Coordinator, business contact information for the head of the public body. The Minister may publish the directory in either print or electronic form.

Access and Privacy, Service Alberta is responsible for coordinating revisions to the Directory of Public Bodies.

**Directory of personal information banks**

**Section 87.1** A *personal information bank* is defined in **section 87.1(5)** as a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Personal information banks have the following characteristics:

- they contain one or more types of personal information;
- they contain information about a group or groups of individuals; and
- the information is organized by a personal identifier or capable of being retrieved by a personal identifier.

Collections of information that are neither organized nor accessible by a personal identifier do not qualify as personal information banks, even if the collection contains personal information. Information that is retrievable only by corporate name does not constitute a personal information bank. Nor does a list of organizations where there is no index or capability of retrieving the names of the contact officers. Collections of personal information that do not qualify as personal information banks must still be managed in accordance with the requirements of the *FOIP Act*.

The directory of personal information banks provides a public listing of all personal information banks in the custody or under the control of a public body. It also provides a public record of the purposes for which this information may be used or disclosed.

The Information and Privacy Commissioner may consider or review a public body's directory of personal information banks if there is a complaint or general investigation relating to the collection, use or disclosure of personal information by a public body.

Further information about personal information banks is available in the *Guide to Identifying Personal Information Banks*, published by Access and Privacy, Service Alberta.

The head of each public body is responsible for maintaining and publishing a directory of its personal information banks, which may be in either printed or electronic form. The required content for this directory is the same for all public



bodies, including local public bodies. The directory of personal information banks must include

- the title and location of the personal information bank;
- a description of the kind of personal information and the categories of individuals whose personal information is included;
- the authority for collecting the personal information in the personal information bank; and
- the purposes for which the personal information is collected or compiled and the purposes for which it is used or disclosed.

**Section 87.1(3)** requires a public body to record any use or disclosure of personal information that is different from those listed in the directory. This notation must be either attached to or linked to the personal information in question, and the new purpose(s) must be included in the next update to the directory.

**Section 87.1(4)** requires the head of a public body to ensure that the directory is kept as current as is practicable.

---

## 2.8 Accessing Manuals and Guidelines

**Section 89(1)** of the Act requires that public bodies make available for inspection by the public any manual, handbook or other guideline used in decision-making processes that affect the public. This provision applies to manuals used by employees when administering or carrying out programs or activities. Rules for program administration, formulae or eligibility criteria for grants or other benefits, guidelines for reviewing applications, and procedures for administering a public program are included. The availability of material that guides decision-making allows members of the public to understand how decisions that affect them are made and opens up the decision-making process to public scrutiny (see *IPC Order F2002-023*).

**Section 89(1)** does not apply to manuals or handbooks that deal only with internal decision-making, such as internal personnel practices or records management guidelines.

There is no requirement under this provision for a public body to provide access to information in a manual that is already available to the public for purchase, as in the case of the Supports for Independence Policy Manual produced by Alberta Employment and Immigration (*IPC Order F2002-023*). There would also be no requirement to provide access to information that is readily available on a public website.

Each public body should provide facilities where the public may inspect manuals, handbooks and guidelines used in decision-making, both at its headquarters and, if reasonably practicable, at other offices of the public body. There are a number of ways to accomplish this. One approach may be to designate space in the office areas of the FOIP Coordinator and appropriate regional contacts. Another is to provide access in an existing library or resource centre.

The term “facility” may include a location such as a reception area, a work station, an office or any other area used for the purpose of providing access to manuals and guidelines. In addition to providing a facility where the public may inspect manuals,



handbooks and guidelines used in decision-making processes, some public bodies are providing access to these records through a website.

**Section 89(2)** provides that manuals, handbooks and guidelines may be reviewed by the public body before being made available for public examination. Any information that would not be disclosed in accordance with the exceptions set out in the Act may be severed.



If information in a manual, handbook or guideline is severed, the record must include a statement that information has been severed and the reason for the severing (i.e. the section number).

Access to manuals and guidelines, facilities for the public to consult these documents, and different ways of providing access are discussed in FOIP Bulletin No. 3: *Access to Manuals and Guidelines*, published by the Access and Privacy, Service Alberta.

## 2.9

### Disclosure to the Commissioner by a Public Body Employee

**Section 82(1)** of the Act provides that an employee of a public body may disclose to the Information and Privacy Commissioner any information which that employee is required, whether under oath or by agreement, to keep confidential, if the employee, acting in good faith, believes that the information

- ought to be disclosed by the head of the public body under the public interest provisions of **section 32**; or
- is being collected, used or disclosed in violation of the privacy provisions contained in **Part 2** of the Act.

The intent of **section 82** is to protect employees. The provision encourages employees to come forward when they honestly believe that the public body for which they work is either ignoring an important public interest by failing to disclose particular information, or failing to meet the obligations to protect personal privacy imposed by the provisions of **Part 2** of the *FOIP Act*.

The Commissioner will seek proof that the employee is *acting in good faith*. This means that the employee has an honesty of intention or honestly believes that he or she is following a lawful path. If the Commissioner is satisfied that the complaint is in good faith, there must be an investigation of the alleged failure to comply with the Act or the need to disclose certain information. The investigator may use all the powers vested in the Office of the Information and Privacy Commissioner to investigate the matter (**section 82(2)** and **(7)**).

The Commissioner must not divulge the identity of the employee except with the individual employee's consent (**section 82(3)**).

Disclosure can occur through written communication with the Commissioner or through a meeting between the employee and the Commissioner or one of the Commissioner's staff who is delegated to undertake the case.

If an employee has acted in good faith, he or she is protected from prosecution under any Act for

- copying a record or disclosing it to the Commissioner; or
- disclosing information to the Commissioner (**section 82(4)**).

An employee acting in bad faith would not be protected from prosecution. *Acting in bad faith* means acting with mischievous, harmful or false intent.

A public body or any person acting on behalf of a public body is prevented from taking any adverse employment action against an employee acting in good faith who

- has disclosed information to the Commissioner under **section 82**; or
- has exercised or may exercise a right under this section (**section 82(5)**).

Any person who contravenes **section 82(5)** is guilty of an offence and liable to a fine of not more than \$10,000 (**section 82(6)**).

---

## 2.10 Liability

### Protection from liability

Under **section 90** of the Act, a public body and all the officials involved in the administration of the Act are protected from liability for damages for

- disclosing or withholding information, or for the consequences of disclosing or withholding information, where a public official has acted in good faith; or
- failing to give a required notice where the public official took reasonable care in giving notice.

---

## 2.11 Offences and Penalties

### Offences and penalties

**Section 91** protects an employee of a public body from adverse employment action as a result of properly disclosing information in accordance with the Act. Anyone who contravenes **section 91** is guilty of an offence and liable to a fine of not more than \$10,000.

**Section 92(3)** is a special provision that was added in 2006 to prevent the disclosure of personal information of Albertans to foreign courts, especially under outsourcing arrangements. This provision makes it an offence to wilfully disclose personal information to which the Act applies

- in response to a subpoena, warrant or order issued by a court, person or body that has no jurisdiction in Alberta to compel the production of information, or
- in response to a rule of court that is not binding in Alberta.

The penalty for this offence is a fine of between \$2,000 and \$10,000 for an individual, and between \$200,000 and \$500,000 for an offender that is not an individual (e.g. a corporation).

**Section 92** of the Act sets out other offences and penalties and requires public bodies to cooperate with the Information and Privacy Commissioner or another person performing duties of the Commissioner.

It is an offence under the Act to

- collect, use or disclose personal information in contravention of **Part 2** of the Act;
- attempt to gain or gain access to personal information in contravention of the Act;
- make a false statement to, or mislead or attempt to mislead, the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or another person under the Act;
- obstruct the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or other person under the Act;
- alter, falsify or conceal any record, or direct any person to do so, with the intent of evading a request for access under the Act;
- fail to comply with an order made by the Commissioner under **section 72** or by the adjudicator under **section 81(2)**; or
- destroy any records subject to the Act, or direct any person to do so, with the intent to evade a request for access to the records.

Public bodies should note that it is an offence to wilfully reveal or wilfully attempt to gain access to the identity of an applicant in contravention of the Act, whether or not the attempt is successful (see *IPC Order 2000-023*).

Although it is an offence to destroy any records subject to the Act with the intent to evade a FOIP request, there is no duty or requirement as to how a public body should structure or maintain its record retention system (see *IPC Order 2000-030*).

In *IPC Order F2002-006*, the Commissioner commented that giving up the custody of a record to an external reviewer for the purpose of avoiding the requirements of the Act was contrary to the spirit of the Act. It appeared that the public body came “dangerously close” to breaching **section 92(1)(e)**.

Failure to comply with a duty imposed by the FOIP legislation or otherwise acting in contravention of the legislation is not an offence unless it is covered under **section 92(1)**.

The Commissioner may find grounds for believing that an offence under **section 92(1)** has occurred in the course of

- a review requested by an applicant or other individual under the Act;
- an investigation under **section 53**; or
- a disclosure to the Commissioner under **section 82** regarding possible failure to disclose in the public interest or regarding a possible violation of **Part 2** of the Act.

Any other failure to comply with the legislation that is not an offence under **section 92(1)** is dealt with by the Commissioner under the normal review and complaints process set out in **Part 5** of the Act or in an investigation under **section 53**.

Any person who commits an offence under **section 92(1)** or **section 91(1)** is liable, upon conviction, to a fine of up to \$10,000 under **sections 92(2)** and **91(2)** respectively. The Commissioner does not impose the fine. The court, under the

*Provincial Offences Procedures Act*, will determine whether or not an offence has been committed and impose any fine (see *IPC Order 99-012*).

In order to support charges under the offence provisions in the Act, the Commissioner would have to be satisfied, on reasonable and probable grounds, that an offence had been committed. The Commissioner would then swear an Information in Provincial Court to that effect and the charge would be heard in that Court (see *IPC Investigation Report 2001-IR-010*).







## 3.

# ACCESS TO RECORDS

---

### Overview

This chapter covers

- the right of access to records;
- what to do when a FOIP request is received;
- how to deal with access requests that include health information if the public body is also a custodian under the *Health Information Act*;
- how to transfer a request;
- response time limits;
- steps in processing a FOIP request;
- how to assess fees; and
- how to manage request files.

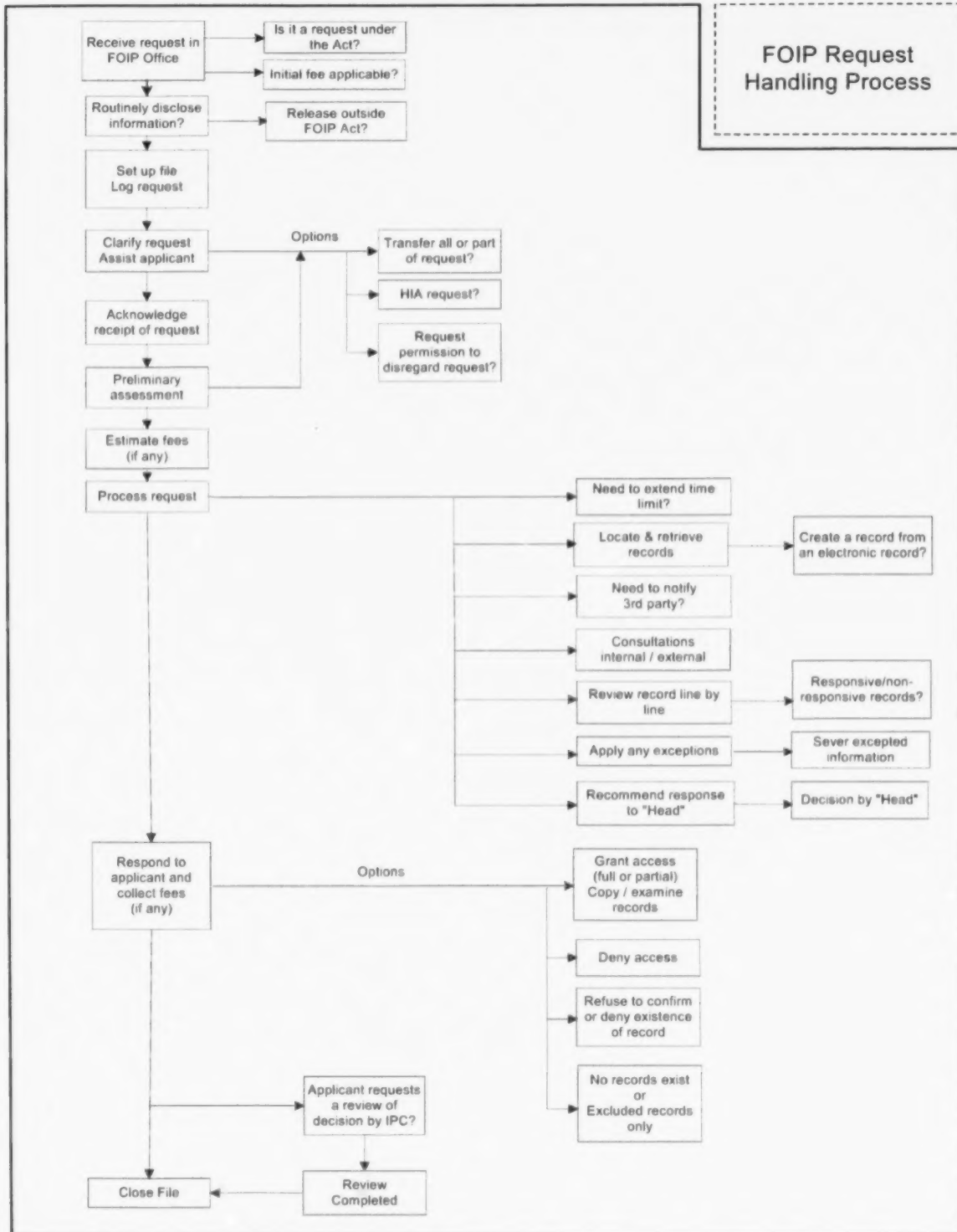
For a diagrammatic overview of the FOIP request-handling process, see the flow chart on the next page.

---

### 3.1 Who has a Right of Access

Any person has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant (**section 6(1)** of the *FOIP Act*).

There are no restrictions as to who may make a request. The applicant can be any person who is residing inside or outside of Alberta, including individuals, corporations, and organizations. The Act does not specify a minimum age, which means that minors may also make requests.



## 3.2

Receiving a  
FOIP Request**Form of the request**

**Section 7(1)** of the Act provides that an applicant must make a request to the public body that the applicant believes has custody or control of the particular record(s).

An *applicant* means a person who makes a request for access to a record under **section 7(1)**.

**Section 7(2)** requires that the request be in writing and provide enough detail to enable the public body to identify the record.

The applicant can use the official request form. A copy of the **Request to Access Information Form** can be found in Appendix 5. Public bodies may either use this form or create one of their own. Alternatively, an applicant may simply write a letter, requesting records and referencing the *FOIP Act*.

**Section 7(3)** permits an applicant to examine the record or to obtain a copy of it, subject to the exceptions in **section 4** of the FOIP Regulation (examination of the record would unreasonably interfere with the public body's operations or might result in the disclosure of information that the public body may or must not disclose).

As long as the original request was properly made, a change to the original terms of the request may be made orally, for example, where the applicant asks to examine records rather than to receive copies (see *IPC Order 99-011*).

**Section 6(3)** states that the right of access is subject to the payment of any fee required by the FOIP Regulation.

**Section 11** of the FOIP Regulation states that an initial fee of \$25 for a one-time request, or \$50 for a continuing request, must accompany a request for general records. There is no initial fee when the applicant is requesting his or her own personal information (**section 12** of the FOIP Regulation).

**Alternative methods of requesting access**

**Section 5** of the FOIP Regulation permits an applicant with limited ability to read English, or an applicant with a physical disability or condition that impairs the ability to make a written request, to make an oral request. The public body should put an oral request into written form and provide the applicant with a copy.

Public bodies should assist individuals seeking records under the Act who are disabled, do not have literacy skills or are otherwise unable to exercise their rights under regular procedures.

In the case of individuals with a hearing impairment, telecommunications devices for the deaf (TDD) should be used. For public bodies that use the Government of Alberta Call Centre, use should be made of the toll-free number 1-800-232-7215, and in Edmonton 780-427-9999, as a telecommunications device for the deaf. For visually impaired applicants, consideration should be given to helping the applicant make a request by assisting in filling out a request form.

A public body only needs to deal with a request in a language in which the body normally conducts business.

Some individuals who live in remote areas may be disadvantaged in comparison with other members of the public in their ability to make a FOIP request. Public bodies should take such situations into account and assist applicants in ways that will enable them to exercise their access rights without excessive cost or delay.

### **Duty to assist applicant**

*Section 10(1)* The head of a public body must make every reasonable effort to assist applicants, and to respond to each applicant openly, accurately and completely. The public body's obligations under **section 10(1)** continue throughout the request process.

*Every reasonable effort* is an effort which a fair and rational person would expect, or would find acceptable (*IPC Order 98-002*).

The Information and Privacy Commissioner has provided a considerable amount of guidance on the duty to assist in Orders issued in a broad range of different cases. These Orders relate to situations that vary widely with respect to the type of applicant, the records involved, and the nature and context of the request. The public body's assistance to the applicant was often just one issue among many to be decided by the Commissioner. How a public body fulfils its duty to assist will vary according to the circumstances of each request, and requires the exercise of judgment in each case.

The duty to assist applies to a request by an applicant under the **section 7** of the Act. This duty also applies to an applicant's request for a fee waiver under **section 93(3.1)**.

The Act does not expressly require the head of a public body to meet the duty to assist under **section 10(1)** when responding to an individual's request for a correction of personal information under **section 36(1)**. While the Commissioner has not ruled on this specific point (see *IPC Order 98-010* on the duty to understand and seek clarification a request), public bodies are advised to consider the purposes of the Act when responding to any request under the Act.

The duty to assist under **section 10(1)** generally arises when a public body is performing activities that are not explicitly addressed in other provisions of the Act (as are, for example, fees and time limits). The most important aspects of the duty to assist are likely to arise in the course of

- providing the information necessary for an applicant to exercise his or her rights under the Act;
- clarifying the request, if necessary;
- performing an adequate search for records; and
- responding to the applicant.

Some of these stages are discussed in detail later in this chapter. This section is concerned with the way in which the duty to assist is engaged when performing these activities. The Commissioner has said that a public body may take into consideration that a sophisticated applicant, such as a professional researcher, may not require the

same level of assistance as another kind of applicant (*IPC Orders 96-014 and 2000-021*).

The duty to assist under **section 10(1)** lies with the head of a public body. In *Order F2007-028* the Commissioner said, with respect to the adequacy of a search – one of the principal aspects of assisting an applicant – that the head, or the head's delegate, should take a supervisory role and be aware of exactly what steps have been taken to locate records.

### ***Providing information necessary for the exercise of rights under the Act***

A public body's duty to assist is engaged when the public body has received an access request under **section 7** of the Act. A public body has no legal obligations under **section 10(1)** until a prospective applicant has submitted a request (*IPC Order 99-011 and IPC Investigation Report 2001-IR-004*).

If there is any uncertainty as to whether a request is a request under **section 7** of the Act, the public body should clarify this with the person making the request and inform the person of the procedure for making a request under the Act (*IPC Investigation Report 99-IR-004 and IPC Order 2001-013*). If there is more than one procedure for obtaining access to information, a public body must inform the applicant of this (*IPC Order 98-002*).

A public body that has received a request for personal information under **section 7** of the Act will not meet its duty to assist under **section 10(1)** unless it responds in accordance with the requirements of **Part 1** of the Act (see *IPC Order 99-035*). If the public body believes it would be more appropriate to disclose personal information under **section 40** of the Act, the public body should advise the applicant of the implications of a decision to proceed in that way (for example, the person would have no right to request a review by the Commissioner). If the person agrees to a different process, the person must withdraw the access request.

### ***Clarifying the request***

Many applicants are unfamiliar with the organization and administrative practices of public bodies. They may not be aware of the process by which a public body reaches or implements a decision or policy, the kind of records that may be generated in the course of that process, and the process of disposing of the records.

The FOIP Coordinator may need to assist the applicant in clarifying the request so that the public body can retrieve records of interest to the applicant (*IPC Orders 97-006 and 98-012*). Clarification of the request may involve assisting the applicant in defining the subject of the request, the specific kinds of records of interest, and the time period for which records are being requested.

The FOIP Coordinator must exercise care in questioning an applicant about the nature of his or her interest in a particular subject. If a question to an applicant could be seen as dissuading the applicant, or as a means of trying to obtain information not needed to process the request, the question should not be asked (*IPC Order 2000-015*). It is generally not necessary to ask why an applicant is asking for particular records.

Narrowing a request as a result of the clarification process can have significant implications for fees. The Commissioner has said that a public body has a duty to engage in the clarification process up to the point when the fee estimate is provided (*IPC Orders 99-011 and 2000-022*). However, a public body has no obligation to request clarification of a request that is, on its face, very clear (*IPC Order 2001-013*).

The process of clarifying requests is discussed in greater detail later in this section.

### ***Performing an adequate search for records***

A public body must conduct an adequate search for records that are responsive to the applicant's request (*IPC Orders 97-006 and 98-012*).

The Commissioner has said that there are two components of an adequate search. The public body must

- make every reasonable effort to search for the actual record requested; and
- inform the applicant in a timely fashion of what it has done (*IPC Orders 96-022 and 98-012*).

A public body must make a reasonable effort to identify and locate records responsive to the request (see *IPC Order 2000-030*). A public body cannot decide not to conduct a search for records on the basis of an opinion that no responsive records exist (*IPC Order 99-021*). In a case where a public body has conducted a previous search in response to another request, if there is any doubt that the request is for substantially the same information, the public body must conduct a completely new search. If the other search was substantially similar but earlier, the public body must search for records that may have been created since the earlier request (*IPC Order 99-021*).

A public body must search all locations, including off-site locations, where records might be found (*IPC Order 99-021*). The search strategy, not the amount of time spent on a search, will determine whether a public body has conducted an adequate search (*IPC Order 99-039*).

A public body is not required to search for records in the custody or under the control of other public bodies (*IPC Orders 97-006, 99-021 and F2003-001*). It is not part of the duty to assist for a public body to inform an applicant of the location of other records (unless the public body knows that records may exist elsewhere), to provide indexes to files that are not required to be located and reviewed as part of the request, or to provide records retention and disposition schedules when they have not been requested (see *IPC Order 99-039*).

The obligation to search for records exists even if the public body believes it would be expensive, difficult and time-consuming to conduct the search. A public body is not required to search electronic back-up records if it does not have the ability to do so, but it may not *choose* not to search back-up electronic records if it has the ability to do so (*IPC Order F2007-028*). The process of searching for and retrieving responsive records is discussed in greater detail in section 3.4 of this chapter.





**A public body must make every reasonable effort to identify and locate records responsive to a request, and provide the applicant with information regarding the processing of the request in a timely manner (IPC Order 98-012).**

### ***Responding to the applicant***

A public body must respond openly, accurately and completely. Even if an applicant has requested records that are not subject to the Act, the public body must respond and inform the applicant that records cannot be obtained under the Act (see *IPC Order 2000-022*).

In a case where more than one public body has received the same request from the same applicant, each public body must respond to the request on its own behalf (see *IPC Order 99-035*).

Copies of records must be legible where possible. When a record is severed, the public body should clearly identify the basis on which the record was severed (*IPC Order F2003-020*).

The duty to assist does not require that public bodies provide medical or legal interpretations of the information in records, or provide information to clarify the information in the records. It is also not necessary to disclose the nature or contents of records that are withheld in a response to an access request (*IPC Order 2001-041*). A public body is not generally required to make an applicant aware of records that may relate to the applicant's request but have not been specifically requested (*IPC Investigation Report 2001-IR-010*).

The process of responding to an applicant is discussed in greater detail in section 3.8 of this chapter.

### ***Acknowledging receipt of request***

The public body should acknowledge receipt of a request. This acknowledgment may indicate that the request

- has been received and processing will commence;
- is incomplete because the initial fee has not been paid and is required before processing can commence; or
- is not clear or precise enough and more information is needed to clarify it before processing can commence.

Under **section 7(2)** of the Act, a request must provide enough detail to enable the public body to identify the record. If processing cannot begin immediately because the request is not clear, an effort should be made to contact the applicant by telephone to resolve any problems quickly. There is no provision in the Act for putting a request on hold pending clarification with the applicant (see "Clarifying requests" later in this section). However, the time limit for responding to the request may be extended

under **section 14(1)(a)** if the applicant does not give enough detail to enable the public body to identify a requested record.

A written follow-up to the initial telephone contact with an applicant is good practice. It will provide a definite reference point as to when processing commenced and a statement of the agreement between the public body and the applicant as to the nature and scope of a request that has been clarified.

**Model Letter A** in Appendix 3 sets out various options for acknowledging receipt of a FOIP request.

### **Continuing requests**

**Section 9** An applicant may ask that a request continue in effect for a specified period of time up to two years. This permits the applicant to continue to receive records concerning a particular subject or issue at regular intervals over time, for example, quarterly.

The head of the public body may choose to accept or reject a continuing request. If the head accepts a continuing request, the public body may determine the schedule for release of records so that it meets both the needs of the applicant and the operational constraints of the public body.

The head of a public body may have grounds for rejecting a continuing request if

- the situation or event that is the subject of the request is not an ongoing matter and there is no basis on which to set up a continuing request; or
- the situation that is the subject of the request is dependent on other actions involving the applicant and the applicant is receiving the information routinely on an ongoing basis.

The Act applies to a continuing request as if a new request were received on each date that processing of an instalment of the request is due to begin. The public body is required to provide the applicant with a schedule indicating the series of dates when the request will be deemed to have been received, and to inform the applicant that he or she has the right to ask the Commissioner to review the schedule. On each scheduled date, the time limit for responding to the request begins again.



The FOIP Coordinator should have a system in place to alert his or her office when a request should be reactivated.

**Section 13(3)** of the FOIP Regulation requires a public body to provide an estimate of the total fees payable over the course of the continuing request. A new fee estimate need not be provided on each of the scheduled delivery dates. Rather, the public body must decide what portion of the estimate will apply to each delivery of records in the continuing request and provide this information to the applicant. To do this, the public body would estimate the total fees payable over the course of the continuing request and decide how much of that estimate is likely to apply to each delivery (see *IPC Order 97-019*).

**Model Letters A and B** in Appendix 3 deal with continuing requests.

### **Request for access to personal information about an applicant**

Individuals may make requests for information about themselves.



The same general conditions that apply to receiving requests for access to general records apply to receiving requests for an individual's own personal information. However, there is no initial fee for requests for an individual's own personal information, and no service fees may be charged except fees for photocopying, if those fees exceed \$10.

It is usually obvious on the face of the request that someone is requesting his or her own personal information. In some instances, however, someone else may be applying on behalf of the individual, and it will be necessary to determine whether the applicant has the authorization of the individual whose information is requested or has some other right under the Act. Common examples of persons who might reasonably request information about another individual are the legal representative of the individual, and the parent of a young child.

At times it may not be clear whether an applicant is requesting his or her own personal information or general records about a subject in which the individual has been involved. The Information and Privacy Commissioner dealt with this issue in *IPC Order 97-003*. A three-part test was applied, whereby the public body would

- consider the wording of the request;
- characterize the request as to whether it is primarily for general records or is for personal information about the applicant; and
- decide whether the records relate to and are responsive to the request being made and whether the preponderance of records relates to the individual.

On this basis, the public body would decide whether it is dealing with a request for personal information.

For further guidance on requests by a representative of an individual for personal information of that individual, see Chapter 2, section 2.5.

### **Request for access to personal information that includes health information**

#### ***For public bodies that are not custodians under the Health Information Act***

For these public bodies, information about an individual's health and health care history that is part of an access request is considered personal information under **section 1(n)(vi)** of the *FOIP Act*.

#### ***For public bodies that are custodians under the Health Information Act***

The definition of record in **section 1(q)** of the *FOIP Act* is the same as the definition of record in **section 1(1)(t)** of the *Health Information Act*. **Section 4(1)(u)** of the

*FOIP Act* says that the *FOIP Act* does not apply to health information, as defined in the *Health Information Act*, that is in the custody or under the control of a public body that is a custodian, as that term is defined in the *Health Information Act* (see *IPC Order F2002-015*).

In the event that a public body subject to both Acts (e.g. the department of Health and Wellness or Alberta Health Services) receives a request for access to an individual's personal information, the rules regarding access to information under the *Health Information Act* would apply to the individual's *health information*. Subject to **section 4(1)(u)**, the rules regarding access to personal information under the *FOIP Act* would apply to the individual's or another person's *personal information*, as that term is defined in **section 1(n)** of the *FOIP Act*.

For example, if a visitor to a hospital was injured during an incident involving a scuffle with hospital security staff and was treated at that hospital, the visitor's health information as a patient of the hospital would be subject to the *Health Information Act* access rules. However, any other personal information about the visitor collected or created by security staff as a result of the incident would be subject to the access rules under the *FOIP Act*. Another example of records that may be subject to the two Acts would be employee records that contain both health information and personal information about an individual.

Under **section 15.1** of the *FOIP Act*, if a request for access to a record is made under **section 7(1)** of that Act, and a part of the record contains information to which the *Health Information Act* applies, the part of the request relating to the health information is deemed to be a request under **section 8(1)** of the *Health Information Act* and the rules in that Act will apply to the processing of that part of the request (*IPC Order F2004-005*).

The applicant must be notified regarding the part of the request that will be processed under the *Health Information Act*, and whether this will affect the timelines for responding. **Model Letter A.1** in Appendix 3 can be used to notify an applicant that part (or all) of a request is being deemed to be a request under the *Health Information Act*. Applying the *Health Information Act* to part of the request should not have an impact on the request process. The processing of access requests under both Acts is similar.

If FOIP requests and *Health Information Act* requests are handled by two different persons or offices within a public body, it is important for the two persons or offices to consult with one another regarding a request for access to records containing both types of information. The public body will have to make decisions regarding the disclosure of records in accordance with the Act that applies to the relevant portion of the records requested.

If both types of requests are handled by the same person or office, a separate file should be opened and a request number assigned for each request. One request would be for access to the individual's personal information and the other request would be for access to the individual's health information.

The **Fee Schedule** in the FOIP Regulation would apply to the personal information requested, except for the portion of the records containing information to which the

*Health Information Act* applies. The Fee Schedule under the Health Information Regulation would apply to the portion of the request related to health information.

Although a public body that is a custodian under the *Health Information Act* will process different portions of an individual's request for his or her own information under both Acts, it may wish to apply the lower fees of the two fee schedules, where possible, unless the majority of the information requested is health information and significant review time will be required. Under section 10(3) of the Health Information Regulation and section 2(o) of Schedule 2 in the Regulation, a fee may be charged for the time it takes to review and determine whether any severing will be required. Under **section 12(2)** of the FOIP Regulation, a fee cannot be charged for this review time.

More information on processing requests under the *Health Information Act* may be found in the *Health Information Act Guidelines and Practices Manual (2006)*, published by Alberta Health and Wellness.

### **Authorization to disregard requests**

**Section 55** In exceptional cases, a public body may ask the Information and Privacy Commissioner to authorize the public body under **section 55(1)** of the *FOIP Act* to disregard certain requests.

The head of a public body may be allowed to disregard a request if it is

- repetitious or systematic in nature, and processing the request would unreasonably interfere with the operations of the public body or amount to an abuse of the right to make requests (**section 55(1)(a)**); or
- frivolous or vexatious (**section 55(1)(b)**).

In considering whether **section 55(1)** applies, the Commissioner has said that he will be mindful of the principles of the *FOIP Act* and the relevant circumstances. A public body must show that either **section 55(1)(a)** or **55(1)(b)** applies to the request (Commissioner's decisions of April 10, 2002 and February 5, 2003).

### ***Repetitious or systematic requests***

A public body may request authorization to disregard repetitious or systematic requests only if processing the request would unreasonably interfere with the operations of the public body or amount to an abuse of the right of access.

A request is *repetitious* when a request for the same records or information is submitted more than once (Commissioner's decision of March 13, 2007).

*Systematic in nature* includes a pattern of conduct that is regular or deliberate (Commissioner's decision of March 13, 2007). The Commissioner found that the submission of five access requests of similar scope over a period of two and a half years was systematic in nature (Commissioner's decision of April 10, 2002).

In determining whether a request is *repetitious*, a public body may not take into consideration attempts to obtain access to the information through means other than the *FOIP Act*. Requests made outside the *FOIP Act*, including requests in the course



of the collective bargaining and arbitration processes, are not relevant to **section 55(1)** (Commissioner's decision of February 5, 2003).

In *Order 2006-028*, the Commissioner was asked in the course of an inquiry for authorization to disregard a request under **section 55(1)**. The Commissioner reiterated that using more than one process to obtain access to records (in this case pre-trial disclosure of documents) did not limit the applicant's right of access under the *FOIP Act*. **Section 3(a)** of the Act specifically allows for more than one process for obtaining access to records. The Commissioner noted in his decision that an authorization to disregard a request was not an Order.

The Commissioner ruled that a fourth request for substantially the same records as in three previous requests was repetitious and an abuse of the right to make requests. The *FOIP Act* was not intended to allow an applicant to resubmit the same or similar access requests to a public body simply because the applicant does not like the information obtained (Commissioner's decision of March 21, 2002).

The Commissioner also ruled that a request was repetitious in a case where the applicant was connected in some material way to, or associated with, a person who had made requests for similar material. The Commissioner found that the applicant's access request was no less an abuse of the right to make requests than if the other person had made the access request. In that case, the Commissioner authorized the public body to disregard future access requests made by those parties, as well as any other requests in which it was clear that the person who made the original requests was the "directing mind" (Commissioner's decision of August 7, 2002).

A request under the *FOIP Act* made after exhausting other avenues for access does not make the FOIP access request *systematic* in nature. That would be contrary to the intent of the *FOIP Act*, which is to grant a right to access to information that is not otherwise available to the person seeking that information (Commissioner's decision of February 5, 2003).

*Unreasonable interference with the operations of a public body* might be demonstrated by showing the impact that particular repetitious or systematic requests are having on the resources needed to respond within a public body, and the actual cost of providing a response.

### ***Frivolous or vexatious requests***

*Frivolous* means of little weight or importance (Commissioner's decision of February 5, 2003).

*Vexatious* means without reasonable or probable cause or excuse (Commissioner's decision of February 5, 2003). A request is *vexatious* when the primary purpose of the request is not to gain access to information but to continually or repeatedly harass a public body in order to obstruct or grind a public body to a standstill (Commissioner's decision of November 4, 2005).

In determining whether a request is *frivolous*, the Commissioner has noted that information that may be trivial from one person's perspective may of importance from another's. In deciding whether a request was frivolous, the Commissioner considered the evidence and found that the applicant perceived the information



sought as a matter of importance and that the focus of the applicant's actions was on the information requested. The Commissioner decided, from an objective point of view, that the access request in question was not frivolous (Commissioner's decision of February 5, 2003; see also Commissioner's decision of November 4, 2005).

The Commissioner has ruled that an applicant's attempts to obtain access to information through means outside the *FOIP Act*, including requests under collective bargaining and arbitration processes, are not relevant in determining whether the applicant's access request under the *FOIP Act* is *vexatious* (Commissioner's decision of February 5, 2003).

The Commissioner has also observed that an institution's subjective view of the annoyance quotient of a particular request is not sufficient grounds for disregarding a request. The fact that a request might result in the disclosure of information that the public body might prefer not to disclose would also not be grounds for relief under **section 55(1)(b)** (Commissioner's decision of February 5, 2003; see also Commissioner's decision of November 4, 2005).

#### ***Effect of an authorization request on time limits***

If the head of a public body asks the Commissioner to authorize the public body to disregard a request for access under **section 7(1)** or a request for correction under **section 36(1)**, processing of the request ceases until the Commissioner has made a decision. If the Commissioner authorizes the head of the public body to disregard the request, processing does not resume (**section 55(2)(a)**). If the Commissioner decides not to authorize the public body's request, processing resumes after the Commissioner advises the head of the public body of that decision (**section 55(2)(b)**).

In a decision on one request for authorization to disregard an access request, the Commissioner authorized the public body to disregard any and all future requests made by the applicant under the *FOIP Act* for a period of three years (Commissioner's decision of March 13, 2007).

See IPC FOIP Practice Note 9: *Authorization to Disregard Request under Section 55*, published by the Office of the Information and Privacy Commissioner, as well as the Commissioner's decision of February 5, 2003, for information regarding the procedure for requesting authorization to disregard a request under **section 55(1)** and each party's right of reply.

#### **Clarifying requests**

Vague or overly general requests may increase workloads and lead to review of information that is of little interest to the applicant. Often requests are broad or vague because the applicant lacks knowledge of the public body, its mandate and programs and the type of records available.

If a request is unclear, the FOIP Coordinator should establish contact with the applicant to better understand what information will satisfy the applicant's needs. If a request does not sufficiently describe the records sought, a public body should advise the applicant and offer assistance in reformulating the request.

**Model Letter A** in Appendix 3 deals with this type of situation. There are several things to keep in mind when seeking to define or clarify a request.

#### ***Release of information outside the FOIP process***

A public body may be able to satisfy an applicant's information needs by providing records that are already publicly available, or that can be made available through a process of routine disclosure. When a FOIP request can be dealt with outside the Act, and if no other fee structure applies, the initial fee may be returned to the applicant, along with a copy of the requested record(s). If there is a procedure in place to refer an applicant to the appropriate program area, the fee should not be returned until the applicant has agreed to have the request handled outside the Act by the program area.

The applicant must agree to withdraw the request; otherwise, the public body is required to respond to it under the Act. In some instances, only part of the information can be routinely released. In such cases, this information may be released and the rest of the request processed under the Act.

#### ***Narrowing a request***

It is important to discuss with the applicant any request that involves a large amount of information or is estimated to require a large amount of search time. In *IPC Order F2007-017*, the Commissioner said that a request for a large number of records resulting in a fee estimate of \$144,000 should have signalled to the public body that clarification of the request was required. The objective of clarifying the request in a case such as this is to narrow the request while still meeting the applicant's information needs. This can result in a reduction of fees and provision of better service, in terms of both time and results.

#### ***Changing the scope***

After discussion of the nature of a request, an applicant will sometimes change the scope of the request. When this occurs, the public body should document the change and send a notice to the applicant (see **Model Letter A** in Appendix 3).

Clarifying a request in relation to a public body's duty to assist under **section 10(1)** is discussed earlier in this section.

#### ***Documenting and tracking requests***

A public body should maintain a tracking system to document all deliberations and decisions regarding the processing of a request and to help ensure that the processing of the request meets the requirements of the Act. This record may become a critical part of the evidence required during a review by the Information and Privacy Commissioner. It can also be of assistance in the processing of subsequent similar requests (see *IPC Order 99-011*).

As provided in **section 3** of the FOIP Regulation, the 30-day time period for responding to requests commences on the day after receipt of a request in the office of the public body designated to receive such requests. This is normally the office of the FOIP Coordinator.

Authorized offices are listed in the directory published on the website of Access and Privacy, Service Alberta ([foip.alberta.ca](http://foip.alberta.ca)) and may be publicized in other ways. Authorized offices are usually the offices of the head of the public body and the FOIP Coordinator.

A request may be delivered to any office of a public body during normal business hours, but the time limit for responding to the request does not commence until the request is received in an office authorized to receive requests.

**Section 3(3)** of the FOIP Regulation requires the public body to have a reasonable system in place to ensure that FOIP requests are forwarded immediately to the office(s) designated to receive and begin processing them. Reasonable steps might include special forwarding instructions to staff in mail rooms within the public body and to staff that open the mail, as well as use of a colour-coded transmittal file. Most importantly, staff should be aware of the urgent nature of FOIP requests and the need to forward them immediately to the FOIP Coordinator.



Offices designated to process FOIP requests should date-stamp all requests on receipt.

Public bodies may use an automated or manual tracking system. An automated tracking system is used by all Government of Alberta ministries and is available for use by other public bodies. This system is most beneficial to public bodies that receive 10 or more requests annually.

When implementing or designing a system, a public body should keep in mind that it must provide the information that the Minister responsible for the *FOIP Act* requires for reporting to the Legislative Assembly on the operation of the Act. Notices regarding reporting requirements are regularly issued to public bodies by Access and Privacy, Service Alberta.

### Transferring a request

There are occasions when an applicant makes a request to one public body that would be more appropriately handled by another public body. This may be the case if the other public body produced the record, was the first to obtain the record, or has custody or control of the record.

A public body has discretion in deciding whether to transfer a request to another public body. The Information and Privacy Commissioner has found no significant relationship between the mandatory duty to assist and the discretion to transfer a request (see *IPC Order 2000-021*).

A request for correction of personal information may also be transferred if another public body originally collected the information or created the record (**section 37**).

If the FOIP Coordinator is aware that part of a request relates to records of another public body, the public body receiving the request should inform the applicant that he

or she can make a request to the other organization for the records relating to another part of the request.

### ***Transfer procedure***

**Section 15(1)** Within 15 days after a request for access to a record is received by a public body, the head of the public body may transfer the request and, if necessary, the record, to another public body if

- the record was produced by or for the other public body;
- the other public body was the first to obtain the record; or
- the record is in the custody or under the control of the other public body.

In *IPC Order 2000-021*, the Information and Privacy Commissioner said that one of the following three conditions must be satisfied for a request to be transferred:

- the public body receiving the transferred record generated the record, whether it created the record itself or instructed an employee or agent to create the record on its behalf;
- the public body receiving the transferred request was the first entity to obtain the record after its creation by another party, whether or not obtaining the record was intentional; or
- the public body receiving the transferred request has custody or control of the responsive record at the time of the transfer of the request.

In addition, the Commissioner said that the Act does not require the public body transferring the request to consult with the public body receiving the request before the transfer is made. In practice, however, it may be useful to consult with the FOIP Coordinator of the other public body before transferring the request.

In many cases, interest in the disclosure of particular records will exist in several public bodies. This might be the case, for example, with requests for the records of interdepartmental or multi-organizational committees, or requests for records relating to budgeting processes and programs in which two or more public bodies are involved.



For the sake of administrative simplicity and good client service, the public body receiving a request that relates to more than one public body should process it, consulting and seeking advice from the other interested bodies, rather than attempting to negotiate a complicated sharing of the request. In such cases, the public body processing the request has the final decision as to what will be disclosed. The applicant should be informed if a public body makes an informal request to another public body to search for records. (*IPC Order 99-021*.)

Where similar requests are directed to a number of provincial public bodies, Access and Privacy, Service Alberta may take a coordinating role. Such coordination involves explaining difficult issues and promoting communication among public bodies. Decision-making about a request will always remain with the public body processing a request.

### ***Transfer of a request for correction***

**Section 37** A public body may transfer a request to correct personal information if

- the personal information was collected by another public body, or
- another public body created the record containing the personal information.

This provision allows the public body that originally collected the personal information or created the records to make the corrections, annotation or linkage required. The onus is then on that public body to inform others to whom the information has been disclosed of its decision about the request.

If the public body decides not to transfer a request for correction, it should consult with any other public body that collected the personal information or created the record containing the information.

### ***Conditions of transfer***

**Sections 15(2) and 37(2)** When a request is transferred, **sections 15(2) and 37(2)** of the Act require the public body that transferred the request to provide notice to the applicant as soon as possible. **Model Letter C** in Appendix 3 deals with notice to an applicant regarding the transfer of a request.

**Sections 15(2) and 37(2)** also require the public body receiving the request to make every reasonable effort to respond to the request within 30 days after receiving it, unless a time extension is sought on one of the grounds set out in **section 14** of the Act.

The public body to which the request is transferred should also acknowledge receipt of the request by writing to the applicant, using **Model Letter A** in Appendix 3.

### ***Consultation***

When a public body receives an access request and the request deals with records that originated in another public body, or with matters in which another public body has a direct interest, it should consult with that public body. This will ensure that all relevant factors are taken into consideration in deciding whether or not to disclose all or part of the records. A public body should also consult with another public body with respect to a request for correction in similar circumstances.

Two public bodies may deal with different aspects of the same matter or policy and may even disagree on policy directions or administrative actions to be taken. The public body receiving the request should ensure that the views of the other body have been taken into consideration in any decision to disclose or to refuse access to all or part of the records concerned.



If more than two public bodies are involved, the consultation process should ensure that all parties are aware of each other's views. Public bodies that regularly need to consult with other public bodies on disclosure in response to access requests may need to set out their procedures for consultation and decision-making in policy.

### 3.3 Response Time Limits

**Section 11(1)** of the Act provides that public bodies must make every reasonable effort to respond to a request no later than 30 calendar days after receiving it, unless

- the time limit is extended under **section 14**; or
- the request is transferred to another public body under **section 15**.

*Every reasonable effort* means the effort that a fair and rational person would expect to be made and would find acceptable. A public body's effort is expected to be thorough and comprehensive (see *IPC Order 98-002*).



When calculating time periods, statutory rules apply. Alberta's *Interpretation Act* says that if a time is expressed to begin after, or anything is to be done before a specified day, the time does not include that day. The 30-day time limit for processing requests is based on calendar days, not working days. The time limit begins on the day after the request is received in a duly authorized office and any initial fee is paid. If a time limit expires on a Sunday or other holiday, the time limit is extended until the next working day.

If the request is incomplete and further information is required from the applicant in order to identify the records sought, a public body should seek this information immediately. The requirement to clarify the request does not change the date on which the time period commences, but may necessitate a time limit extension.

#### **Deemed refusal**

**Section 11(2)** Failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under **section 14**, can be treated by the applicant as a decision to refuse access to the record(s). Failure to respond to a request may be reviewed by the Information and Privacy Commissioner (see *IPC Order 99-039*).

#### **Time limit extensions**

**Section 14** A public body may extend the time limit for responding to a request. The circumstances in which an extension is permitted are limited, and, in some cases, the permission of the Information and Privacy Commissioner is required.

A public body may extend the time limit for responding by up to 30 days, allowing a total period of up to 60 days, in any of the following circumstances.

- The applicant does not give enough detail to enable the requested records to be identified. This may be because the request is vaguely worded or, for some other



reason, the record is impossible to locate from the description provided. In this case, clarification is needed from the applicant.

- A large number of records are requested or must be searched, or a large number of records must be reviewed, and responding within 30 days would unreasonably interfere with the operations of the public body. This type of request will usually result in discussions with the applicant to try to narrow the scope of the search.
- More time is needed for the public body to consult with other public bodies, other levels of government, or third parties. This provision applies to third party consultations as required under **section 30** of the Act (which may take up to 20 days), consultation with other governments under **section 21** (for which there is no specified time limit), and consultation with other public bodies (where the public body has no legislated power to compel a timely response).

If a public body believes that it still cannot complete processing of the request within a 30-day extension period, the public body may ask the Commissioner for a longer extension.



**Public bodies must continue to process a request while awaiting the Commissioner's response to an extension request.**

**Section 14(1)(d)** allows for a time limit extension when a third party asks the Commissioner to review a head's decision on a request. In order to allow time for the third party to ask the Commissioner to review the decision, an additional 20 days may be required. For further information on time limit extensions related to the third party notice process, see FOIP Bulletin No. 10: *Third Party Notice*, published by Access and Privacy, Service Alberta.

If a review by the Commissioner is requested by a third party, the records requested by the applicant must be withheld until the review is completed and any Order issued.

**Section 14(3)** allows the head of a public body to extend the time limit for responding to a request in accordance with **section 14(1)(a) to (d)**, without seeking the permission of the Commissioner, even if the cumulative effect of granting allowed extensions takes the time period beyond 60 days. This may occur if the need to consult with a third party is not recognized until late in the processing of a large request. In this case, the extension is needed to provide sufficient time to comply with the notification provisions of the Act (see *IPC Investigation Report 2000-IR-001*).

The public body should consider all factors relating to the need for a time limit extension before extending the time limit. Common factors include

- the amount and type of detail required from the applicant to clarify a request;
- the breadth and complexity of the request, the number of records requested, and the number of files that must be searched to find the requested records;
- the number and complexity of consultations required with external organizations, such as other public bodies or other levels of government;

- the quantity and type of records requiring review by other public bodies (public bodies are not third parties for the purposes of notices and time limits under **sections 30 and 31**; however, they may reasonably be expected to respond in a timely manner); and
- the amount of time needed for the Commissioner to deal with a request for review (the Commissioner's office should be consulted on this matter).

The public body should indicate to the applicant the specific provision that it is relying upon for the time limit extension (see *IPC Investigation Report 2000-IR-001*).

The Act does not provide for extensions for other administrative reasons, such as

- consultations within the public body after the records have been located; or
- working conditions arising from sickness, staff absence or vacation, or staff workloads.

#### **Limits on extensions**

A public body should make every effort to plan the processing of a complicated request so that there is no more than one extension. A public body may, on its own authority and within the time limits under **section 14(1)**, extend the time limit for another 30 days or less to enable the head to comply with the requirements of **section 31**.



**If a public body is able to determine that responding to the request will require more than a total of 60 days, the head is required to ask the Commissioner for permission to extend the time limit beyond the original 30 days. This must be done in writing, and normally within the original 30-day time limit. The reasons for the extension must meet the conditions of section 14(1).**

A letter requesting an extension by the Commissioner should set out the specific reasons why a period greater than 60 days is required to process the request. The letter should propose a reasonable period of days for producing a response.

Normally, if a public body has already taken a 30-day extension under its own authority, it should not seek a further extension from the Commissioner. However, this may be done in exceptional circumstances, where complications not originally contemplated when planning the response process arise. An example might be where a public body has already claimed an extension of 30 days because of the need for extensive consultation. On the 45th day, as a result of that consultation, it discovers additional records that have to be searched and from which responsive records will be retrieved. In this case, the public body would request the permission of the Commissioner to extend the period for response to the applicant.

**Section 14(2)** of the Act also provides for a public body, with the Commissioner's permission, to extend the time limit for responding to a request in the following circumstances:

- multiple concurrent requests are made by the same applicant, or
- two or more applicants who work for the same organization, or who work in association with each other, make multiple concurrent requests.

This provision acknowledges the difficulty that a public body may have if one or more applicants make a number of requests at the same time.

**Section 14(2)** applies to any time limit extension, even if only an additional 30 days are required. A public body requesting an extension from the Commissioner under **section 14(2)** should provide information about the multiple concurrent requests, as well as any of the factors set out in **section 14(1)** that will affect the processing of the requests.

If the Commissioner refuses to grant a time limit extension under **section 14(2)**, the public body may consider each request separately to determine whether an extension is needed under **section 14(1)**.

A public body must document the reasons for a time limit extension. This documentation will be helpful in case of a complaint by the applicant to the Commissioner.

#### **Notification**

**Section 14(4)** This provision of the Act requires a public body to notify the applicant that an extension is being taken, the reason for it, the date when a response can be expected, and that the applicant has the right to make a complaint to the Information and Privacy Commissioner about the extension.

**Model Letter D** in Appendix 3 deals with time extensions. This notice should be given as soon as it is apparent that the request cannot be processed within the initial 30-day time period.

When a request for an extension is made to the Commissioner, the notice should be sent to the applicant before the Commissioner's final decision has been made as to whether the extension will be granted.

After investigating a complaint about a time limit extension, the Commissioner may either confirm or reduce the extension, as provided in **section 72(3)(b)**.

#### **Impact of third party notice on response times**

When a public body gives notice to a third party under **section 30**, the deadline for a final response to an applicant must take into account the time required to allow the third party to respond. No decision may be made before either 21 days after the day notice is given or the day a response is received from the third party, whichever is earlier. The public body should notify the third party as soon as possible after receiving a request in order to minimize the delay in responding.

Giving a third party notice is discussed in Chapter 5.

### **Day of response**

Under Alberta's *Interpretation Act*, if the day a response is due falls on a holiday or a day when the office of a public body is closed, then the response is due on the next business day. For example, a third party has 20 days to request a review by the Information and Privacy Commissioner after the public body has notified the third party of a decision regarding access to records affecting the third party. If the 20th day falls on a Sunday, the third party would have until the next business day (Monday) to request a review. The public body could not release the records that were the subject of the third party notice to the applicant until the following day (Tuesday).

The head of the public body is responsible for determining whether the office that is authorized to handle requests is closed. For example, a school board is still responsible for processing requests when offices of the administration are open but individual schools are closed. A process must be established in such cases to ensure records are retrieved.

If a public body, such as a small municipality, completely closes its office for staff vacations, then the completion of the request will be affected and may not commence until the first working day after the office reopens.

---

### **3.4 Processing a FOIP Request – Search and Retrieval**

In responding to FOIP requests, it is important that a public body clearly assign responsibilities for the various processing steps. This section outlines the assignment process and describes the responsibilities of program areas in a decentralized organizational model, where retrieval and review of records is performed in program areas and the office of the FOIP Coordinator carries out management of the final decision-making. In a centralized model, the office of the FOIP Coordinator will carry out all the duties outlined in this chapter. (Conducting an adequate search for responsive records in relation to a public body's duty to assist under **section 10(1)** is discussed in section 3.2 of this chapter.)

Public bodies should develop procedures for processing requests and for doing so within applicable time limits and in accordance with the requirements of the Act. Public bodies should also create and retain documentation on their processing of requests. The forms provided in Appendix 5 may be used or adapted for this purpose.

Model **FOIP Request Charts** are provided in Appendix 4.

### **Receipt of a request**

Once a request is received in the office of the FOIP Coordinator, it should be registered. The request should then be placed in a request file and details of the request forwarded to any program area that may have custody or control of requested records. The office of the FOIP Coordinator can record this assignment of responsibility in the request tracking system.

The request should be accompanied by a **FOIP Transmittal Memorandum** and **Access Request Processing Summary** for recording all activities and the time involved in processing the request, in order to document these activities and assess

the appropriate fees. A model **FOIP Transmittal Memorandum** and an example of an **Access Request Processing Summary** are included in Appendix 5.

The identity of the applicant should be disclosed only

- to those officials and employees of the public body who have a need to know it in order to carry out their job duties; and
- to the extent necessary to carry out the public body's functions in processing the applicant's request.

For instance, where the request is for general records, the FOIP Coordinator should forward only the request for records and not the name of the applicant or other identifiers to program areas within the public body (see *IPC Investigation Report 98-IR-009* and *IPC Order 99-021*).

An access request contains recorded information about an identifiable individual. The personal information of the applicant can be disclosed to another employee of the public body only if the employee has a need to know that information (see *IPC Order 2000-023*).

### **Locating, retrieving and copying records**

A public body must make a reasonable effort to identify and locate records responsive to the request (see *IPC Order 2000-030*).

A search for responsive records must consider all records, as defined in the Act, including all electronic records that are in the custody or under the control of the public body.

A public body must search all locations, including individual offices, central active files and off-site locations, where records might be found (see *IPC Order 99-021*).

The search for electronic record may include electronic information management systems, business applications, shared directories, e-mail systems, websites, collaboration sites, and social media.

Electronic devices, including laptops, BlackBerries and other PDAs, cellular phones, portable media and storage devices, may need to be searched as well.

A public body may also have to search for responsive records under its control that are in the hands of a third party (see *IPC Order F2002-014*). This would include records in the possession of a contractor. A public body is not required to search for records in the custody or under the control of other public bodies (*IPC Order 97-006*).

Records and information management staff may be able to identify finding aids that will assist in locating relevant records in paper and electronic formats. Finding aids may include classification schemes, records retention and disposition schedules, records inventories for particular repositories, and indexes to specific systems.

A public body must be prepared to support claims for the adequacy of a search with evidence as to how the public body conducted its search in the particular



circumstances (*IPC Orders 98-003 and 2000-030*). In *IPC Order 2007-029*, the Commissioner stated that evidence as to the adequacy of a search should cover the following:

- the specific steps taken by the public body to identify and locate responsive records,
- the scope of the search conducted (e.g. physical sites, program areas, specific databases, off-site storage areas),
- the steps taken to identify and locate all possible repositories of relevant records (e.g. keyword searches, records retention and disposition schedules),
- who did the search, and
- why the public body believes no more responsive records exist than what has been found or produced.

The program area is normally responsible for locating and retrieving all records relevant to a request that are in its custody or control. Speed and accuracy are essential in identifying, locating, retrieving and, where appropriate, copying records relevant to a request (where a request is for a large number of records, it may be appropriate to delay making copies).

Staff in search locations should be told to keep track of and report on the amount of time spent on locating and retrieving records. If the search is expected to involve a large number of hours, the FOIP Coordinator should be notified. The FOIP Coordinator may want to contact the applicant to discuss whether the scope of the request, and resulting fees, could be reduced.

Once the records have been located, either the program area or the office of the FOIP Coordinator should prepare them for review for responsiveness and the possible application of exceptions. In cases where the request is very clear, this may involve the copying and numbering of all records responsive to the request. Where the request is less clear, or where there are a large number of records, it may be appropriate to defer any copying until after the preliminary assessment by the FOIP Coordinator.

#### ***Disposition of records***



**Public bodies must not dispose of any records relating to a FOIP request after it is received, even if the records are scheduled for destruction under an approved records retention and disposition schedule.**

This includes any e-mail and transitory records relevant to the request that may exist at the time the request is received. In effect, the receipt of a FOIP request freezes all disposition action relating to records responsive to the request until the public body has responded to the request, the Commissioner has disposed of any complaint or request for review, and all time limits relating to the exercise of rights by parties have passed.

For continuing requests, disposition action freezes at the point when the request is reactivated in accordance with the agreed schedule.



The file transmitting the request to the program area should include a reminder that it is an offence to destroy any record, or to direct another person to do so (**section 92(1)(g)**), or to alter, falsify or conceal any record, or to direct another person to do so (**section 92(1)(e)**) in order to evade a request for access to records. These offences are punishable by a fine of up to \$10,000.

Where records have been destroyed prior to the receipt of a request, in accordance with an approved records retention and disposition schedule, the public body's response to the applicant should indicate that the records have been destroyed, quoting the relevant destruction certificate numbers for the records (see *IPC Order 99-021*).

When records have been transferred to the Provincial Archives of Alberta or the archives of the public body, the request should be transferred to the archives for processing, unless some other arrangement between the two organizations exists (see *IPC Order 96-022*).

### **Preliminary assessment**

After the records have been retrieved, the next step is a preliminary review of the records by the FOIP Coordinator. In larger public bodies, the FOIP Coordinator might involve a program contact or other person knowledgeable about the subject matter and records.

There are a number of matters to consider at this stage.

- Does it appear that all relevant records, including electronic records, have been located and do they appear to respond to the request?
- Are there any records referenced in the request or the located records, such as attachments, that have not yet been located?
- Are any of the records excluded from the scope of the Act under **section 4** or subject to other legislation that prevails over the *FOIP Act*?
- Should all or a portion of the request be transferred to another public body that produced the record, was the first to obtain the record, or has the record in its custody or under its control?
- Does it appear that records may be found in program areas other than those already identified, and should the search be widened?
- Is consultation needed with other program areas within the public body? Responsibility for ensuring that these consultations occur should be clearly assigned.
- Is external consultation needed with other public bodies and levels of government? Responsibility for conducting these consultations should also be clearly assigned.
- Do the records contain third party business information or personal information that may require third party notification?
- Will the time required to respond to the request likely exceed the 30-day time limit? Are there grounds for an extension of the time limit?

- Will fees in addition to the initial fee (if applicable) be assessed for the processing of the request?

From this preliminary review, the FOIP Coordinator may, depending on the level of delegation, either recommend or undertake actions related to

- the transfer of all or part of the request;
- the extension of time limits;
- third party notification; or
- the assessment of fees.

Each of these activities involves a notice to the applicant. Notices are considered in this publication as follows:

- extension of time limits is discussed in section 3.3 of this chapter;
- third party notification is discussed in Chapter 5;
- transfer of requests is discussed in section 3.2 of this chapter; and
- assessing fees is discussed in section 3.5 of this chapter.

### Notices

Various notices are required under the Act. Of particular importance are those that are sent

- to inform an applicant of a fee estimate;
- to report to an applicant about the progress of a request (e.g. any extension of the time limit for responding);
- to notify a third party (a business or an individual) that information provided by the third party or personal information about the third party has been requested, and that an opportunity is being provided for comment on whether the information should be disclosed; and
- to advise the applicant of the decision on the disclosure and, if access is being granted, provide information about access to the requested records.

**Section 83** of the Act provides for the manner of giving notice. **Section 83** is discussed in section 2.6 of Chapter 2.

Public bodies should assess the circumstances requiring the notice and choose the most effective and economical approach. If a public body is sending a notice by fax or other electronic means, care should be taken to prevent unauthorized disclosure of third party information (see *IPC Investigation Report 2001-IR-001*).

The **Model Letters** in Appendix 3 provide examples and options for all the notices required under the Act.

---

### 3.5 Assessing Fees

The *FOIP Act* allows public bodies to charge fees to help offset the cost of providing applicants with access to records. The Act provides for a fee structure that is intended to support effective provision of FOIP services.

**Section 93** establishes that

- a public body may require an applicant to pay fees for services as provided for in the FOIP Regulation (**section 93(1)**);
- for personal information, fees are restricted to the cost of providing a copy of the information (**section 93(2)**);
- if fees are required under **section 93(1)**, an estimate of the total fee must be prepared by the public body for the applicant before providing the services (**section 93(3)**);
- an applicant may, in writing, request that the head of a public body excuse the applicant from paying all or part of the estimated fees (**section 93(3.1)**);
- the head of a public body may excuse an applicant from paying all or part of a fee if, in the opinion of the head,
  - the applicant cannot afford the payment or for any other reason it is fair to excuse the payment; or
  - the record relates to a matter of public interest, including the environment or public health or safety (**section 93(4)**);
- the decision of the head of a public body on a fee waiver request must be communicated in writing to the applicant within 30 days of receiving the request for a fee waiver (**section 93(4.1)**);
- the fees referred to in **section 93(1)** must not exceed the actual costs of the services provided (**section 93(6)**).

**Section 95(b)** enables local public bodies to establish their own fee structures provided they follow **section 93** of the Act and do not exceed the fee structure set out in the FOIP Regulation. This must be done through a bylaw or, where applicable, other legal instrument by which the local public body acts.



**GST is not charged on fees for processing FOIP requests.**

**Fees for general records**

**Section 11(4)** and **Schedule 2** of the FOIP Regulation set out the maximum fees that may be charged for processing a general access request.

The head of a public body may require an applicant who makes a request under the Act to pay fees for the following services:

- locating and retrieving a record;
- producing a record from an electronic record;
- preparing a record for disclosure (to cover the time taken to physically sever the record);
- providing a copy of a record;
- creating a new record from an electronic record under **section 10(2)** of the Act;

- supervising the examination of an original record, and
- shipping.

No fee may be assessed for time spent in reviewing a record to determine whether or not all or part of it should be disclosed.

If new records have to be created from an electronic record, the public body may use acceptable industry standards to ensure accuracy and completeness of the records, process the information according to its usual procedures, and charge for these services as a part of its fee. If the public body uses a reasonable process, there is no obligation under the Act to change the process simply because an applicant believes a faster or more efficient method to complete the task may exist.

In the event of a review by the Commissioner, the public body has the burden of proving that it has reasonably calculated the fee estimate (see *IPC Orders 99-014* and *F2002-005*).

The fee provision is discretionary, but normally fees will be assessed for all general requests under the Act. Fee waiver provisions are set out in **section 93(4)** of the Act. The FOIP Regulation (**Schedule 2**) sets out the maximum fees that may be charged. Public bodies may choose to charge less than these rates, but not more.

A person who makes a request for access to a general record that is not a record of the applicant's own personal information is required to pay

- an initial fee of \$25 at the time that a one-time request is made; or
- an initial fee of \$50 when a continuing request is made.

This initial fee covers the work involved in registering the request, locating and retrieving records, and, in some instances, providing access to records. For simple, straightforward requests involving a small volume of records, it will be the only fee paid. For complex requests or requests involving a large volume of records, the initial fee would probably only cover the preparation of a fee estimate. Additional fees will likely be required.

No additional fees are charged unless the amount of fees required to process the request for general records, as estimated by the public body to which the request has been made, exceeds \$150. When the amount estimated exceeds \$150, the total amount is charged to the applicant.



**Processing a FOIP request for general records must not commence until the initial fee has been paid.**

### **Fees for personal information**

**Section 12** of the FOIP Regulation sets out the fees that an individual may be charged for accessing his or her own personal information.

In the case of a request for an applicant's own personal information, an applicant will pay only copying fees, and then only when those fees exceed \$10, as determined by the public body in accordance with the rates established in **Schedule 2** of the FOIP Regulation. Subject to the fee waiver provision (**section 93(4)**), when the fee exceeds \$10, the total amount will be charged to the applicant.

For more information on assessing fees when dealing with requests that contain both personal information and health information under the *Health Information Act*, see section 3.2 of this chapter.

### Fee estimates

**Section 13** of the FOIP Regulation governs the provision of fee estimates under the Act.

When a public body provides a fee estimate to an applicant in accordance with **section 93(3)** of the Act and **section 13** of the FOIP Regulation, the estimate should provide a breakdown of all applicable fees that will be charged to the applicant. The estimate should use the language of the Act and Regulation; for example:

- the time required and cost for searching for, locating and retrieving the record(s);
- the time required and cost for preparing and handling the record(s) for disclosure; and
- the cost of producing a paper copy of the record(s) in the required format (e.g. black and white up to 8½" x 14").

Where the Regulation allows for the "actual cost" of the service, the public body should indicate the basis on which it has estimated the actual cost (e.g. time required and rate per ¼ hour for computer programming).

In the case of a request for access to a record of the personal information of the applicant, the public body must only include the cost of copying the record.

In the case of a continuing request, the estimate must include the total fees payable over the time span of the continuing request (see *IPC Order 97-019*). The notice to the applicant about fees should include

- a request that at least 50% of the estimate be paid in advance of the request being processed, or in the case of a continuing request, a request that at least 50% of the estimate for the first instalment be paid in advance of the request being processed;
- a statement that the applicant has 20 days to inform the public body that the estimate is accepted and to pay the deposit; and
- a statement that the applicant has the right to ask the head of the public body to excuse all or part of the fee and may request a review by the Information and Privacy Commissioner if the fees are considered too high or otherwise inappropriate, or if a request for a fee waiver has not been granted.

**Model Letter E** in Appendix 3 may be used to provide this notice. The notice gives the applicant the basis on which to accept the fees or take other action. The applicant might narrow the request, review original records, which would incur supervision



costs but would cut down on copying costs, seek a fee waiver, or request a review of the fees by the Commissioner under **section 65(1)** or **section 53(2)**.

No further processing takes place until one of the following events occurs:

- a letter from the applicant agreeing to the charges and attaching payment of the deposit is received in the authorized office (the applicant has up to 20 days to accept the fee estimate);
- written notification from the applicant modifying the request, and establishing a new basis for assessment of fees, is received in the authorized office;
- the public body agrees to a request for a fee waiver; or
- the Commissioner carries out a review and decides whether the fees are appropriate, or whether the head of the public body has appropriately exercised his or her discretion regarding a request for a waiver of fees, as applicable.

An applicant has up to 20 days to indicate whether or not the fee estimate is accepted.

More detailed guidance on estimating fees is provided in FOIP Bulletin No. 1: *Fee Estimates*, published by Access and Privacy, Service Alberta.



**Fee estimates are not binding. However, a public body should do its best to estimate what the fees will be. The public body can revise its estimate in the course of processing the request. If the estimate is too high, the public body must refund any fees paid by the applicant that exceed the actual cost of processing the request. If a fee estimate is too low, the public body has the discretion to request additional fees from an applicant. The fact that fees will be higher must be addressed with an applicant as soon as it becomes apparent, and not be left to the end of the processing period.**

### **Deposits and payment of fees**

Processing of a request ceases once a notice of estimate has been forwarded to an applicant and recommences immediately upon

- receipt of an agreement to pay the fee; and
- receipt of at least 50% of any estimated fee that exceeds \$150 (FOIP Regulation, **section 14(1)(a)**) or, in the case of a continuing request, receipt of at least 50% of the portion of the estimate applicable to the delivery of the instalment of the request to be processed (FOIP Regulation, **section 14(1)(b)**).

The balance of any fee owing is payable at the time the records are provided to the applicant (FOIP Regulation, **section 14(2)**).

If the amount paid is higher than the actual fees required to be paid, the balance paid will be refunded. The initial fee is not refunded in these circumstances (FOIP Regulation, **section 14(3)**).





**The applicant should not be provided with access to a record until all fees owing for the processing of the request have been paid (section 6(3) of the Act).**

Local public bodies should arrange for fees paid under the Act to be handled in the same way as other revenue.



**Government ministries must deposit revenue collected from FOIP fees to IMAGIS Account Code 446425.**

### **Excusing or waiving fees**

**Section 93(4)** provides that a public body may excuse the applicant from paying all or part of a fee (i.e. grant a fee waiver) if, in the opinion of the public body

- the applicant cannot afford the payment or for any other reason it is fair to excuse payment; or
- the record relates to a matter of public interest, including the environment or public health or safety.

Normally, an applicant will take the initiative in requesting a fee waiver, usually at the time of submitting the request itself. A public body must consider the request for a fee waiver from an applicant at the time it is made. If a request for a fee waiver is part of the FOIP request, the public body will consider it when it is preparing a fee estimate and decide whether or not the request meets any of the criteria for excusing fees and, if it does, whether or not a fee waiver is merited.

An applicant must make a request for a fee waiver in writing (**section 93(3.1)**).



**The public body does not need to waive all fees if it decides to grant a request to excuse payment. It can consider reducing the fee by a part of its total or not charging for certain services.**

If an applicant has requested a fee waiver, and the public body does not grant it, the public body must notify the applicant that he or she may ask the Commissioner for a review of this decision (**section 93(5)**).

The decision of the head of a public body concerning a request for a fee waiver must be communicated in writing to the applicant within 30 days of receiving the request for a fee waiver (**section 93(4.1)**).

When making a decision on a fee waiver request, the head of the public body must make the decision on a case-by-case basis. The head of a public body will not have properly exercised his or her discretion if a fee waiver request is denied on the grounds of a standing policy rather than on consideration of the merits of the individual case (*IPC Order F2006-001*).

The Commissioner may conduct a review of the decision by the head of the public body under **section 65(1)**. **Section 72(3)(c)** enables the Commissioner to make a fresh decision on fees in the appropriate circumstances, for example, where new evidence not available at the time of the public body's decision is presented by the applicant at an inquiry (see *IPC Order 2000-008*).

### **Grounds for excusing fees**

**Section 93(4)** establishes the criteria for excusing payment of all or part of a fee.

#### ***Applicant cannot afford to pay***

**Section 93(4)(a)** The head may excuse payment if the applicant cannot afford the payment. The onus of substantiating financial hardship falls on the applicant (*IPC Order 96-002*). The applicant may be required to supply documentation of income and expenses (*IPC Orders 99-012* and *2000-011*).

The public body should assure the applicant of the confidentiality and security of financial information submitted to the public body in support of a fee waiver request.

When making a decision on grounds of financial hardship, a public body may take into consideration a range of factors, including the scope of the request and amount of the estimated fee; whether the applicant is prepared to pay a portion of the fee; and whether the applicant is willing to work with the public body to narrow the scope of the request and to accept other options. *IPC Order 2007-016* provides a summary of the principles that apply to fee waivers based on financial hardship.

#### ***Other reasons why it is fair to excuse payment***

**Section 93(4)(a)** The head of a public body may excuse the applicant from paying all or part of a fee if, in the opinion of the head, it is fair to excuse the payment for any reason other than financial hardship.

**Section 93(4)(a)** may be used by a public body when it wishes to grant a fee waiver on its own initiative.

The reasons to excuse fees on grounds of fairness may relate to any number of matters. The following are some examples of circumstances where the fees may be waived on grounds of fairness.

- The public body has assessed fees where the records provide little or no information (see *IPC Order 99-027*).
- The public body has failed in its duties in processing the access request, for example, by conducting an inadequate search for records or allowing undue delay (see *IPC Order 99-039*).
- More than one applicant made the same or a similar request at around the same time, and it would not be fair for the public body to collect the total estimated amount of fees from both applicants or to charge the first applicant substantially more than the second (see *Adjudication Order 2*).

Some of the following factors may also be relevant to a decision on fairness.

- The records are critical for the applicant to exercise his or her rights, or are directly related to an individual's personal financial or health management.
- A person has a legitimate reason to request the personal information of another individual, but cannot exercise that individual's rights under **section 84** (if the individual requested the information the request would be subject to copying fees only).
- If the public body set aside the fees associated with records that would likely be withheld, the fee would be likely to fall below the \$150 threshold, or marginally above the threshold.

**Record relates to a matter of public interest**

**Section 93(4)(b)** The head of a public body may excuse the applicant from paying all or part of a fee if, in the opinion of the head, the record relates to a matter of public interest, including the environment or public health or safety.

The concept of public interest has been explained in a number of Commissioner's Orders (*IPC Order 96-002*; reiterated in *IPC Orders 2001-023* and *F2003-011*). The term "public" may be applied to *everyone* and *anyone*. The term "interest" can range between the sense of individual curiosity and the notion of interest as a benefit. The Commissioner has reasoned that the weight of public interest depends on a balancing of the relative weight afforded to curiosity and benefit, and to a broad versus a narrow public. The Commissioner has also said that public interest is not confined to environmental and public health and safety issues.

It should be noted that the criteria for determining public interest under **section 93** are not the same as for the Act's provision for disclosure in the public interest (**section 32(1)(b)**). **Section 32(1)(b)** overrides all other provisions of the Act, including its provisions for the protection of personal privacy. Public interest in **section 32(1)(b)** must be narrowly interpreted, limited to compelling public interest. **Section 93(4)(b)**, on the other hand, is intended to support access rights, and is therefore interpreted more liberally. (See *IPC Orders 98-011*, *98-019* and *2000-031*.)

This category of fee waiver is generally appropriate where there is a public interest in disclosing all or part of a record. This occurs when the information is likely to contribute significantly to public understanding of the operations or activities of the public body, or is of major interest to the public, as in the case of information about the environment or public health or safety.

In *IPC Order 96-002*, the Information and Privacy Commissioner listed thirteen "criteria" for determining public interest. In *Order F2006-032*, the criteria were revised. There are now just three criteria; some of the original thirteen criteria have become "relevant considerations."

- Will the records contribute to the public understanding of, or to debate on or resolution of, a matter or issue that is of concern to the public or a sector of the public, or that would be, if the public knew about it?

The following may be relevant considerations:

- Have others besides the applicant sought or expressed an interest in the records?
- Are there other indicators that the public has or would have an interest in the records?

In *IPC Order F2007-020*, the uniqueness of the public body's program, the amount of public funds involved and the errors that allegedly occurred in administering the program were found to be indicators that the public has or would have an interest in the records. This weighed in favour of disclosure.

- Is the applicant motivated by commercial or other private interests or purposes, or by a concern on behalf of the public or a sector of the public?

The following may be relevant considerations:

- Do the records relate to a conflict between the applicant and government?
- What is the likelihood the applicant will disseminate the contents of the records?

The fact that a print media applicant would publish the information in the records was a factor that favoured disclosure. However, requests for a fee waiver by the media are to be determined on the specific facts of the case. Public interest and not public curiosity is the standard to be applied (*IPC Order F2007-020*).

- If the records are about the process or functioning of government, will they contribute to open, transparent and accountable government?

The following may be relevant considerations:

- Do the records contain information that will show how the Government of Alberta or a public body reached or will reach a decision?
- Are the records desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to scrutiny?
- Will the records shed light on an activity of the Government of Alberta or a public body that has been called into question?

The disclosure of records relating to security breaches and errors in the distribution of rebate cheques was desirable for the purpose of subjecting the activities of the government to public scrutiny, and shedding light on a process that had not been addressed in the government news releases or on the program website (*IPC Order F2007-020*).

Public bodies should consider these questions when exercising their discretion as to whether to waive or reduce fees. A public body may ask an applicant requesting a fee waiver in the public interest to provide information relating to any of the points that appear relevant to the records under consideration.

**Section 93(4)(b)** requires a public body to form an independent opinion about whether a record relates to a matter of public interest (see *IPC Order 2001-023*). A public body could determine, after considering all relevant facts and circumstances and the principles and objects of the Act, that a record relates to a matter of public

interest, even though the applicant may have failed to establish a public interest in the record (*IPC Order F2003-011*).

If the Commissioner conducts a review of a decision not to grant a fee waiver in the public interest, the public body may find it helpful to show that it applied these criteria in making its assessment.

Fee waivers are discussed in more detail in FOIP Bulletin No. 2: *Fee Waivers*, published by Access and Privacy, Service Alberta.

### 3.6 Abandonment of Requests

Often, it is clear when an applicant has decided not to pursue a FOIP request. An applicant will indicate either in writing or on the telephone an intention not to proceed with the request. This may be for a variety of reasons. For example, the applicant has found that the information is available outside the FOIP process or no longer needs the information.

Sometimes situations will arise where an applicant simply ceases to respond during the processing of a FOIP request. No indication is given that the applicant has decided not to pursue the request. He or she simply does not respond to queries from the public body.

When this latter situation occurs, **section 8** of the Act sets out provisions for declaring a request abandoned. The public body must have contacted the applicant in writing and either sought further information that is necessary to process the request or requested payment of or agreement to a fee.

If the applicant does not respond within 30 days of being contacted, the public body can advise the applicant, again in writing, that the request has been declared abandoned. A specific date for this declaration should be included in the notice. This notice must state that the applicant can ask for a review by the Commissioner of the decision.

In most cases, abandonment of a request occurs before processing of the request is completed. However, in some cases, an applicant abandons a request after processing is completed. If the public body has responded to the applicant's request, stating where, when and how access will be given; and has requested that the applicant contact the public body about viewing the records, and the applicant does not respond within 30 days, then the public body can advise the applicant that the request has been declared abandoned. The procedure outlined above will apply to such requests.

It is good practice for a public body to keep the file active for a further 60 days in order to allow time for the applicant to request a review by the Commissioner.

**Model Letter F** in Appendix 3 deals with this type of situation.



### 3.7

#### Processing a FOIP Request – Reviewing and Preparing Records for Disclosure

#### **Line-by-line review of records**

Once the preliminary assessment has been completed, the various administrative matters have been sorted out and any necessary consultations are under way, a knowledgeable staff member from the program area or, in centralized systems, the office of the FOIP Coordinator, will need to review the documents line by line.

A line-by-line review is essential to comply with the principle of severability set out in **section 6(2)** of the Act. This provision grants an applicant a right of access to any record from which excepted material can be reasonably severed. Chapter 4 deals with the guidelines for the application of the exceptions to the right of access.

With input from the program or business unit responsible for the records, the reviewer should be able to form an assessment of the likelihood of harm as a result from release of particular information and identify factors to be taken into consideration when exercising discretion to withhold information. During a line-by-line review, the office of the FOIP Coordinator may identify additional requirements with respect to third party notices or consultations.

#### **Documentation**

The reviewer should document exceptions to be invoked, actions to be taken, reasons for each decision, and recommendations for responding to the request.

A model **Access Request Processing Summary** is provided in Appendix 5. Public bodies may adapt this form for their internal use.

Thorough documentation at this stage will ensure that the public body has the information required to assess recommendations from the program area and to reach final decisions relatively quickly. Documenting the decision-making process minimizes duplication of effort and ensures that the public body is in a position to explain decisions both to the applicant and to the Information and Privacy Commissioner, if there is a request for a review.

#### **Reviewer's recommendations**

The reviewer should prepare a summary of recommendations that identifies

- specific records or parts of records that are excluded from the scope of the Act;
- specific records or parts of records to which mandatory or discretionary exceptions to disclosure apply, with the reviewer's recommendations and reasons with respect to the discretionary exceptions (for guidance on the exercise of discretion, see Chapter 4); and
- other general factors that may be pertinent in reaching a decision on a response to the request.

This summary will provide the basis for a discussion between the office of the FOIP Coordinator and the program area of recommendations for a report on the response. At this stage, any legal advice needed to resolve issues arising from the request should be sought. Also, any interpretative or policy issues that need to be raised should be identified and consultation undertaken.



The report should contain

- a log of staff time spent locating, retrieving, copying, and reviewing the records;
- a summary of file systems, offices, and records storage facilities searched;
- copies of records responsive to the request (where this is possible and appropriate given the volume of records or the fact that the applicant wishes to view the original records);
- documentation of the line-by-line review, identifying the specific information in the retrieved records that it is proposed to except from access;
- a summary of third party notices sent and responses received;
- a summary of results of consultations with other public bodies and levels of government; and
- a summary of recommendations for release or refusal, including brief background information to explain decisions.

The **Access Request Recommendation Form** in Appendix 5 serves as the authority to produce the response to the applicant and should be signed by the official delegated to make this decision on behalf of the public body.

### Creating a new record

Under **section 10(2)** of the Act, a public body must create a new record from an existing electronic record if

- the record is in the custody or under the control of the public body;
- the new record can be created using the public body's normal computer hardware and software and technical expertise; and
- creating the record would not unreasonably interfere with the operations of the public body.

This is the only case where the *FOIP Act* requires a public body to create a new record.

An applicant may ask a public body to create a record from a record in electronic form for the purpose of obtaining information in a form that does not currently exist within the public body. For example, a public body may have a database management system that generates certain reports, but not a report of the kind wanted by the applicant. If the public body is able to produce a report setting out the information in the form requested by the applicant, the public body must do so, provided this can be done using the public body's normal computer hardware and software and technical expertise. The public body can charge for this service in accordance with **Schedule 2** of the FOIP Regulation.

A public body may determine how best to respond to the applicant's request. For example, the Information and Privacy Commissioner found that a public body's record-generating process was reasonable, even though the applicant believed that it was more time-consuming and thus more expensive than necessary. In that case, the public body had to locate the file and complete a verification process to ensure accuracy and completeness of the information (see *IPC Order 99-014*).

If a record cannot be created using the public body's normal computer hardware and software and technical expertise, the public body is not required to create the record. For example, a public body was not obliged to create an electronic copy of requested e-mail messages because exceptions applied to the records and the public body did not have the technical capacity to sever the records electronically. In that case, the public body was required to provide paper copies of the records (*IPC Order F2002-017*).

A public body is not required to create a record if to do so would unreasonably interfere with the operations of the public body. For example, the Commissioner found that a health care body was not required to create a record when that would require an extensive amount of time, a significant amount of staff resources, and would result in specialists being removed from patient care (*IPC Order 2001-016*).

In another situation, when an applicant requested an electronic record of information contained in computer logs, the public body determined that the computer processing would have a significant negative effect on the data centre. The Commissioner considered the detailed technical evidence and agreed that processing the request would unreasonably interfere with the operations of the public body. The Commissioner decided that the public body did not have to create any record, electronic or paper (*IPC Order F2002-017*).

The office of the FOIP Coordinator should consult with both the program and information technology areas to assess the time and resources that would be required to create the record and the impact that this use of resources would have on its day-to-day activities.

The creation of a new record from data that can be manipulated may have advantages for both the public body and the applicant in some instances. Excepted material can sometimes be easily suppressed, saving time-consuming severing procedures. The applicant is also often very satisfied with the information received because it is in a more usable or understandable form. However, an applicant may have concerns about the integrity of the data.

Care should be taken to explain the methods used to create a record and what information is being suppressed so that the applicant does not think that information is being manipulated to alter the record or place a different perspective on it.

### **Responsive information**

Information or records are responsive to an applicant's access request if the information or records are reasonably related to the request (see *IPC Orders 97-020* and *2001-037*). A public body's response to a request should include all records that are reasonably related to the request and no records that are not relevant to the request. Non-responsive records should be set aside, and non-responsive parts of records should be identified before making working copies and before any severing of the copies.

A public body may wish to apply the following approach to determine which records may be non-responsive to the request:

- retrieve all records generally responsive to the request (i.e. everything related to the issue, question or topic);
- carefully analyze the text of the request and consult further with the applicant if necessary;
- carefully examine all retrieved records to determine which ones are reasonably related to the request; and
- set aside material that is clearly not on the topic of the request and records that fall outside an established date range, if there is one; identify any non-responsive parts of records.

Public bodies may have different approaches to the retrieval of records. However, it should not be necessary for the FOIP Coordinator to retain significant amounts of non-responsive material in the request file. Consideration should be given to returning anything that is clearly non-responsive to the program area.

A public body is entitled to treat the date of receipt of a request as the outer time limit for the access request. The Commissioner has said that it would be unworkable for an applicant to request an open-ended time frame (*IPC Order 2000-020*).

The fact that an applicant already has or knows the substance of the information, or has knowledge of the contents of a record, does not mean that the record can be considered non-responsive. The public body's obligation is to address the applicant's entire request (see *IPC Order 98-005*). However, a public body and an applicant may agree not to make copies of such records in order to save costs.

Removal of non-responsive information must occur before severing takes place using the exceptions in the Act (see *IPC Order 97-020*).

A public body can remove information as non-responsive only if the applicant has requested specific *information*, such as his or her own personal information. If an applicant asks for a record, then the whole record is generally considered responsive and any part of the record that is not to be disclosed must be severed on the basis of the exceptions in the Act (see *IPC Order 99-002*). Despite this general rule, the public body may treat portions of a record as non-responsive if they are clearly separate and distinct and entirely unrelated to the access request (see *IPC Order 99-020*).

Certain records that are identified as responsive to a request may be records that are excluded from the scope of the Act under **section 4**. If a public body chooses to provide access to excluded records, it should be made clear to the applicant that the records are outside the scope of the Act. For information about responding to a request involving excluded records, see section 3.8 of this chapter.

### Severing information

Many records contain both information that can be disclosed and other information that may or must be withheld. When information that falls within an exception can reasonably be severed from a record, an applicant has a right of access to the remainder of the record (**section 6(2)**).

When a discretionary exception applies, a public body must use discretion not only in applying the exception, but also in determining how much of the information is severed. This is the reason for undertaking a line-by-line review of a record. The object of severing is the use of discretion to disclose as much information as possible, without causing the harm contemplated by the exception.

The only exception to this procedure is when using the exception for legal privilege. When legal privilege applies to a record, the whole record is withheld.

In *IPC Order 96-017*, the Commissioner discussed the two-step process a public body must follow when arguing for a discretionary exception in an inquiry. A public body must first provide evidence on how a particular exception applies, and second, how the public body exercised its discretion. A public body must show that it took into consideration all of the relevant factors when deciding to withhold the information. It must show that it considered the purposes of the Act, one of which is to allow access to information.

#### ***Information that must or may be severed***

All records, regardless of format or previous actions taken, must be reviewed for exceptions and severed accordingly. The fact that an applicant may already have obtained copies of some of the records outside the FOIP request process does not eliminate the need for severing to respond to a request (see *IPC Order 98-016*).

When severing is required for information stored on specialized media, technical expertise should be sought as to the best way to excise information while recording that severing has been done and for what reason.

In some cases, a record cannot be severed (e.g. most records subject to legal privilege). The public body will have to refuse access to the whole record and must be prepared to demonstrate to the Information and Privacy Commissioner the technical reasons underlying the inability to sever. Examples include personal information of two or more individuals so intertwined in a record that severing would be extremely difficult, or when, after severing, the severed record would make no sense or is meaningless (see *IPC Orders 96-019, 2000-023, 2000-028 and 2001-001*).

#### ***Procedures***

During the line-by-line review of records pertinent to a request, the reviewer should identify portions of paper-based records that probably should be withheld, the section of the Act that supports the non-disclosure, and the rationale for using that exception. The reviewer should also keep notes about information in other media that may qualify for an exception. The review and severing of records may require a significant amount of time. The review procedure should ensure that all records responsive to the request are reviewed.

The objective in severing is to remove from the body of a record only the information that meets the conditions for an exception. The Act requires that all information in a record that is responsive to the request, and which will be intelligible to the applicant after severing, be disclosed.

The process is governed by reasonableness, and the public body exercises discretion in determining whether or not discrete portions of information contribute to the overall understanding of the subject matter at issue.

As a best practice, employees should be encouraged to draft documents with information that the public body may wish to except, such as recommendations and advice or personal data, segregated in particular parts of the document. This will make the severing process more efficient. Once the decision has been made to apply an exception to a record and a further decision is made regarding how much information will be severed, the office of the FOIP Coordinator can use one of the following severing methods:

- use of non-permanent white tape over the excepted portion of a copy of the record and recopying to obtain the record to be released;
- use of liquid eraser over the excepted portion of a copy of the record and recopying to obtain the record to be released;
- use of a photocopying machine with editing features suitable for severing; or
- use of redaction software to edit the severable information.



Whatever method of severing is selected, the office of the FOIP Coordinator must ensure that none of the excepted information remains visible. For this reason, the use of markers is not recommended.

### ***Indication of severing***

A public body that refuses access to a record or part of a record must tell the applicant the reasons for the refusal and the provision of the Act on which the refusal is based (**section 12(1)(c)(i)**). The public body must provide a description of the responsive records, without revealing information that has been withheld. At a minimum, the public body should tell the applicant the number of records withheld and the number of pages within each record. The public body must provide the section number of any exception used to withhold information (*IPC Orders F2004-026 and F2007-013*).

Section numbers may be provided either in the space left after the severing or in the margin closest to the severed information. Where one or more entire pages have been removed, the public body must indicate the number of pages severed, along with the section numbers of the exception(s) used to sever the information.

In *IPC Order 2000-014*, the Commissioner found that a public body had not properly responded to the applicant under **section 12(1)** because it had not notified the applicant that 72 pages of records had been severed. In cases where a single page or a continuous sequence of pages has been completely severed, the exception(s) applied and the pages to which any exceptions were applied should be listed in the response letter or collated on a single page. It is neither necessary nor helpful to provide applicants with multiple blank pages.

In some cases, particularly cases involving law enforcement information or personal information about a third party, placing the section number in the space of the



severed information may itself reveal or imply information that, if disclosed, could cause harm to the law enforcement matter or be an unreasonable invasion of a third party's personal privacy. In these circumstances, a public body may omit section numbers on the severed pages and list the relevant exceptions to disclosure in the letter of notification.

Indicating why information was severed from records helps an applicant understand the public body's decision to refuse access to all or part of a record and assists in the event of a review by the Commissioner of the public body's decision. See IPC FOIP Practice Note 2: *Informing the Applicant of Grounds for Refusal*.

A public body that refuses to confirm or deny the existence of a record under **section 12(2)** is not required to tell the applicant the reasons for the refusal and the provisions of the Act on which the refusal is based.

### **Maintenance of copies**

A public body should keep a file for each request processed. This file should include the original request, internal and external correspondence, an unmarked copy of the responsive records, and a copy of the severed documents released to the applicant. A third copy of the responsive records is also helpful to be used as a working copy.

This practice assists the public body in the event of a review by the Information and Privacy Commissioner. The file may also be helpful to the FOIP Coordinator with respect to requests for the same or similar records in the future. However, unless the new request is made shortly after the original, there is still a need to review the records again (see *IPC Order 99-021*). The passage of time and any changes in the context surrounding the records may result in more information being disclosed. Each FOIP request needs to be processed as a separate request and decisions need to be made in relation to the particular circumstances that apply at the time of the request.

This does not mean that every request is unique. A public body may recognize a pattern of similar requests and plan for them. It may be possible to create easily severable documentation that can be routinely disclosed. This might be done either because the information is in high demand or because disclosure of the information supports overall accountability for a program or activity. In some cases, active dissemination may also be warranted. See section 2.4 of Chapter 2 for further information on routine disclosure and active dissemination.

---

### **3.8 Responding to an Applicant**

**Section 12(1)** of the Act provides that an applicant must be told

- whether access to the requested record or part of it is granted or refused;
- if access is to be granted to the record or part of it, where, when and how access will be given; and
- if access is to be refused, the reason for refusal and the section(s) of the Act on which this is based, the name and contact information of an employee who can explain the reasons for the refusal, and that the applicant may ask for a review of that decision by the Information and Privacy Commissioner.



In its response to an applicant, the *FOIP Act* does not require a public body to answer questions about the record or to clarify what is written. For example, in *Order F2002-025*, the Adjudicator found that the public body met its duty to an applicant when it gave the applicant complete, unsevered copies of the records he had requested.



**When providing an applicant with access to his or her own personal information, a public body must be satisfied that the individual receiving the information is the individual the information is about or an authorized representative of that individual.**

A public body should verify the identity of before giving an individual access to personal information (e.g. by asking for some form of valid photo identification, such as a driver's licence), especially if the information is at all sensitive.

For information on the exercise of rights by representatives, see section 2.5 of Chapter 2.

Responding to an applicant in relation to a public body's duty to assist under **section 10(1)** is discussed in section 3.2 of this chapter.

### **Model responses**

The applicant must be provided with a response to a request. **Model Letters G, H, I, and J** in Appendix 3 provide guidance and options for drafting the various types of final responses to FOIP requests.

In all cases when access is refused, where the record is excluded from the Act, or where the public body refuses to confirm or deny the existence of a record, the response letter must state that, if the applicant requests a review of the decision by the Information and Privacy Commissioner, he or she should provide the Commissioner with

- the request number assigned by the public body,
- a copy of the decision letter, and
- a copy of the original request.

Although the Act does not require *written* notification of the right to request a review, the Office of the Information and Privacy Commissioner recommended that a public body revise its response letter to include this notification (see *IPC Investigation Report 2001-IR-004*).

Generally, the response letter should address the outcomes of the search and review of records in response to a request.

### **Record does not exist**

If the public body cannot locate records responsive to the request, even after contacting the applicant to clarify or reformulate the request, a letter should be sent

informing the applicant of that fact and of the steps taken to attempt to find records. Where a record has been destroyed prior to receipt of the request, information should be provided on the date of destruction and the authority for carrying it out (e.g. the appropriate records disposition number or authorization).

### **Access is granted**

If the public body determines that the information falls within the scope of the Act, and the information does not qualify for any exception, or that it qualifies for a discretionary exception but the public body has used its discretion in favour of disclosing the information, the letter to the applicant will say that access is granted.

Some requests will involve records that take little time to review or are easily disclosable. In these instances, the public body may disclose available records as soon as possible, rather than waiting until all records are ready for disclosure. This situation may occur when some records are ready for disclosure and other records have been sent to third parties for consultation.

When records are disclosed in stages, it may not be clear when the 60-day period for requesting a review by the Commissioner would begin. The Commissioner has not commented on this issue to date, but it should be noted that the *FOIP Act* does not contemplate partial or interim disclosure. Under **section 12(1)(c)**, if some of the records disclosed early have been severed, the applicant must be told that he or she has a right to ask for a review of the decision to apply an exception.

Arguably, the time period under **section 65** for requesting a review of that decision would begin when the applicant has been notified of the decision to disclose some records on an interim basis. However, in the interests of providing the applicant with the longest opportunity to request a review of any decision regarding disclosure of records, it is likely that the Commissioner would determine that the 60-day review period would commence on the date on which the public body sends notice to the applicant of its decision regarding the final disclosure of records.

The applicant will have indicated, in accordance with **section 7(3)** of the Act, whether he or she wishes a copy of the record or to examine the original record. If the request is for a copy and it can be reasonably reproduced, **section 13(2)** of the Act requires that the copy be included in the package. This will be done only if the balance of the fees has been paid.



**A public body must collect all outstanding fees before releasing the records to the applicant.**

See section 3.5 of this chapter for information on assessment of fees.

If it is not possible to include the records with the response letter, **section 13(2)(b)** requires that the applicant be given the reason for the delay and told where, when and how the copy will be provided. The most likely cause of delay is that the applicant must pay outstanding fees before access is provided.

In some instances, the applicant may have asked to examine a record but the record cannot be reasonably severed for examination, or the record is in a format that does not readily lend itself to examination (e.g. a microfilm with much excepted material on it). In these instances, the public body may choose to provide a copy of the record to the applicant. **Section 4** of the FOIP Regulation covers these situations.

A public body cannot attach conditions to the disclosure of records or control the use of those records after disclosure. However, other laws may apply to subsequent use of the information.

### **Excluded records**

If the public body determines that all or some of the records are excluded from the scope of the Act under **section 4**, the public body should notify the applicant that the record or information is excluded and that the applicant cannot obtain access to the record(s) under the *FOIP Act*. The letter should cite the specific exclusion in **section 4** that applies, and state that the applicant has the right to ask the Information and Privacy Commissioner to review the decision of the public body that the specified exclusion in **section 4** of the Act applies.

A record responsive to a request may be excluded from the application of the Act, but a public body may nevertheless choose to provide access to it outside the Act. In such cases, a public body should consult with any affected parties. For example, if the record was created by or for an Officer of the Legislature or an MLA, the Officer of the Legislature or the MLA concerned should be consulted.



In instances where access is provided to an excluded record, it is important that the letter of response inform the applicant that the record is excluded, citing the provision of **section 4** that applies, and indicating that the public body has chosen to provide access to the record outside the Act.

### **Access refused**

If the public body determines that the information falls within a mandatory exception, the information falls within a discretionary exception and the decision is to refuse access, or the information lies outside the scope of the Act, the response letter to the applicant should state

- the reasons for refusal and the sections (i.e. the specific subsections and paragraphs) on which the refusal is based;
- the name, title, business address and business telephone number of the FOIP Coordinator or other official who may be able to answer questions the applicant may have; and
- that the applicant has the right to request a review of the decision under **section 65(1)** of the Act and that this request must be made within 60 days after notification of the decision (see *IPC Order 2000-014*).

### ***Refusal to confirm or deny existence of record***

In certain cases, a public body may believe that an applicant's knowledge that a record exists may cause harm to a law enforcement matter (**section 20**), may pose a danger to an individual's or the public's safety (**section 18**) or would be an unreasonable invasion of a third party's personal privacy (**section 17**). **Section 12(2)** of the Act permits the public body to refuse to confirm or deny the existence of a record in these cases (see *IPC Orders 98-009, 2000-004 and 2000-016*).

**Section 12(2)** does not apply to records protected by other exceptions, such as the legal privilege exception (see *IPC Order 2000-015*).

If a public body refuses to confirm or deny the existence of a record containing information specified in **section 12(2)**, the public body does not have to tell the applicant the exception(s) it relied upon to refuse to confirm or deny the existence of the record. However, in the event of a review by the Commissioner, the public body would be required to provide the Commissioner with information regarding which exceptions it relied upon (see *IPC Order 2006-012*).

If the Commissioner is asked to review the public body's decision, the Commissioner must not disclose whether the information exists. In cases where **section 12(2)** has been applied improperly, the Commissioner has ordered the public body to respond to the applicant's request without relying on **section 12(2)**.

### **Request file**

When a public body has responded to the applicant, the FOIP Coordinator should ensure that the public body request file is complete and includes

- all internal and external correspondence;
- copies of records reviewed;
- copies of all records that were released, either severed or complete, to the applicant; and
- any other information documenting the request management process.

---

## **3.9**

### **Completion of Request and Closure of Request File**

#### **Completion of request**

For the purposes of tracking a request and ensuring that the time limits under the Act are met, the processing of a request is complete when the public body has sent its response under **section 12(1)** to the applicant.

However, from a records management perspective, the request file would not be closed until after any balance of fees owing is paid and, if access is granted, the records have been disclosed to the applicant.

Although a request file may be closed after records have been disclosed, the retention period for a request file would only begin after the last recorded activity on the file. It is therefore a good practice to keep a request file active for 60 days after the response has been sent to the applicant in order to allow time for a request for a review by the Information and Privacy Commissioner. If a review is requested, the file will be reopened and remain open until the review process is complete. In the same way, if a

public body sends a notice to an applicant declaring a request abandoned, the file would not be closed and the retention period would not start until after the time period for requesting a review of that decision has passed.

### **Closure of file**

The following may help in determining when an access request file is completed for the purposes of tracking the request, and when the request file may be closed for records management purposes. For a more complete discussion on determining when an access request file is completed after a third party notice process has begun, see Chapter 5.

When an applicant abandons or withdraws an access request, or the request can be processed outside the Act, the request is considered to have been completed on the date the public body sends a letter to the applicant confirming that the applicant has withdrawn the request, declaring the request to be abandoned, or advising the applicant that the request will be handled outside the Act.

When there are no records responsive to an access request, the request is considered to have been completed on the date the public body notifies the applicant in writing that there are no responsive records.

When an access request does not require a notice under **section 30**, the request is considered to have been completed on the date the public body notifies the applicant in writing of its decision under **section 12(1)** (the date on which the letter setting out the public body's decision is sent to the applicant).

When notice is given under **section 30** and the public body decides not to grant access, the request is considered to have been completed on the date the public body notifies the applicant of its decision pursuant to **section 31** (the date on which the letter setting out the public body's decision is sent to the applicant).

When notice is given under **section 30** and the public body has notified the third party and the applicant that it has decided to grant access, the request is considered to have been completed on the 21st day after that notice, if it is determined that the third party has not requested a review, when the records subject to the third party notice could be disclosed to the applicant.

When notice is given under **section 30** and the public body has notified the third party and the applicant that it has decided to grant access, and the third party requests a review of this decision, the file is not considered closed. The retention period for the file does not begin until the matter has been resolved through the review process (e.g. the public body has been notified that mediation was successful). If the Commissioner issues an Order following an inquiry, the file is not closed until the Commissioner confirms that the public body has complied with the order. If the public body disagrees with the Order and applies for judicial review, the file is not closed until the judicial review process is completed, any reconsideration by the Commissioner is completed, and the public body has complied with any order.



### **Retention of file**

Once the file is closed, as indicated above, the public body must retain the file for at least one year to meet the retention requirements of **section 35(b)** of the Act. There may be value in keeping some request files for longer than one year if, for example, the issue that prompted the request is ongoing or key process decisions are noted in the file.

In addition to meeting the requirements of the *FOIP Act*, a public body must also comply with its records retention and disposition schedule. For public bodies that are subject to the Records Management Regulation under the *Government Organization Act*, this is the *Administrative Records Disposition Authority* (ARDA), published by Records and Information Management, Service Alberta, or another schedule approved by the Alberta Records Management Committee (ARMC).

Local public bodies must not transfer, store or destroy request records except in accordance with a bylaw, resolution or other legal instrument by which the local public body acts, or, if no such instrument exists, except as authorized by the governing body of the local public body (**section 3(e)**).

Under **section 92(1)(g)**, it is an offence to wilfully destroy any records subject to the Act, or direct another person to do so, with an intent to evade a request for access to the records. A person who contravenes this section is guilty of an offence and liable to a fine of not more than \$10,000.





## 4.

## EXCEPTIONS TO THE RIGHT OF ACCESS

## Overview

This chapter covers

- the mandatory and discretionary exceptions to the right of access;
- the harms test;
- the exercise of discretion;
- how to apply each exception; and
- when an exception does not apply.

## 4.1

## Introduction

**Section 6(1)** of the *FOIP Act* allows any person a right of access to records in the custody or under the control of a public body, including a record containing personal information about the individual requesting the information.

This right of access does not apply to records that are excluded under **section 4** of the Act or where a provision of other legislation takes precedence over the *FOIP Act*. The exclusions from the Act are discussed in section 1.5 of Chapter 1 and the paramountcy provision in **section 5** is explained in section 1.6 of Chapter 1.

The right of access is also subject to limited and specific exceptions that are set out in **sections 16 to 29** of the Act. The exceptions in the *FOIP Act* all have specific criteria that need to be fulfilled before an exception may be applied.

This chapter explains the various exceptions that require or allow a public body to refuse to disclose information to an applicant who makes a request under the Act.



**A basic principle of the *FOIP Act* is to give the public access to the records of a public body. Any exceptions to the right of access should be applied in a limited and specific way to provide as much access to information as possible.**

Generally, an applicant has a right of access to all or part of any record that is the subject of the request. Refusal to disclose all or part of a record will occur only where the Act provides a specific exception that applies to all or part of a record.

A record cannot be withheld simply because it may contain sensitive or embarrassing information. As well, access cannot be denied because disclosure may expose the public body to liability. Each record must be carefully reviewed, in consultation with public body staff knowledgeable about the record's content and context, to determine whether an exception in the Act applies.

Public bodies should interpret the exception provisions narrowly. Only the specific information to which an exception applies may be withheld under that exception. If

the records are subject to the Act and no exception applies, the information must be disclosed.

More than one exception may apply to all or part of a record. A public body should take into account all relevant factors when considering whether an exception to an applicant's right of access applies to a record. No further exceptions can be applied once the Information and Privacy Commissioner has made a decision on those that have been applied. However, the Commissioner will apply any mandatory exceptions that have not been applied by the public body (see *IPC Order 98-020*).

The exceptions may apply to requests for general information and to requests from an individual for his or her own personal information.

The majority of requests for review to the Commissioner under **section 65** of the Act arise from refusal to provide access. Public bodies should be prepared to document and defend their decisions not to disclose specific information.

### **Mandatory and discretionary exceptions**

There are two types of exceptions under the Act – mandatory exceptions and discretionary exceptions.

#### ***Mandatory exceptions***

Mandatory exceptions begin with the phrase “the head of a public body must refuse to disclose.” If information falls within a mandatory exception, a public body must refuse to disclose all or part of the record as required. Public bodies must review all of the criteria and weigh all of the relevant factors relating to a mandatory exception before deciding whether the exception applies.

The only case where information that falls within a mandatory exception *can* be disclosed is where **section 32** of the Act requires disclosure in the public interest. In this case **section 32** overrides the exception. For further information on disclosure in the public interest, see Chapter 6.

The mandatory exceptions to disclosure are as follows:

- disclosure would be harmful to the business interests of a third party (**section 16(1)**);
- the information is about a third party and is in a tax record (**section 16(2)**);
- disclosure would be an unreasonable invasion of a third party's personal privacy (**section 17**);
- the information is in a law enforcement record and its disclosure would be an offence under an Act of Canada (**section 20(4)**);
- the information would reveal Cabinet or Treasury Board confidences (**section 22**);
- records relating to an audit by the Chief Internal Auditor that are created by or for the Chief Internal Auditor (**section 24(2.1)(a)**);
- disclosure would reveal information about an audit by the Chief Internal Auditor (**section 24(2.1)(b)**) and



- the information is subject to legal privilege and relates to a person other than a public body (**section 27(2)**).

In addition, information must not be disclosed if the disclosure is prohibited by another enactment (Act or regulation) of Alberta that prevails despite the *FOIP Act* (**section 5**) (see section 1.6 of Chapter 1 on paramountcy).

### **Discretionary exceptions**

Discretionary exceptions to the right of access permit a public body to decide whether or not to withhold all or part of a record. Discretionary exceptions commence with the phrase “the head of a public body may refuse to disclose.” There are eleven discretionary exceptions:

- disclosure harmful to individual or public safety (**section 18**);
- confidential evaluations (**section 19**);
- disclosure harmful to law enforcement (**section 20(1)**);
- disclosure harmful to intergovernmental relations (**section 21**);
- local public body confidences (**section 23**);
- advice from officials (**section 24(1)**);
- disclosure harmful to the economic or other interests of a public body (**section 25**);
- testing and audit procedures (**section 26**);
- legal and other privileged information of a public body (**section 27**);
- disclosure harmful to the conservation of heritage sites, etc. (**section 28**); and
- information that is or will be available to the public (**section 29**).

A decision to apply a discretionary exception requires two steps:

- a factual determination must be made as to whether information falls within the category of information that may be withheld from disclosure; and
- the head of the public body must exercise his or her discretion as to whether information should be withheld.

### **Exercise of discretion**

The exercise of discretion is fundamental to applying the Act. It requires the head, or staff member delegated to exercise the discretion of the head, to weigh all factors in determining whether or not information that qualifies for a discretionary exception should be withheld.

The exercise of discretion is not a mere formality. The public body must be able to show that the records were reviewed, that all relevant factors were considered and, if the decision is to withhold the information, that there are sound reasons to support the decision.

In *IPC Order 2000-021*, the Commissioner stated that legislated discretion amounts to the power to make a decision that cannot be determined to be right or wrong in an objective sense. Discretion amounts to the power to choose a particular course of

action for good reasons and in good faith, after the decision-maker has considered the relevant facts and circumstances; the applicable law, including the objects of the Act; and the proper application of the law to the relevant facts and circumstances.

If there is a request for review, the Commissioner decides whether or not an exception applies in a particular circumstance. If a discretionary exception has been properly applied, the Commissioner cannot overrule the head's decision. The Commissioner can, however, require the head to reconsider a decision if it appears that the obligation to exercise discretion has been disregarded, or where discretion has been exercised without due care and diligence or for an improper or irrelevant purpose (see *IPC Order 96-017*).

It is up to the head of a public body to determine whether or not to apply a discretionary exception. If the public body exercises its discretion and decides not to apply a certain exception when it is processing the applicant's request, the Commissioner has no authority to consider the application of that exception at the request of an affected party (*IPC Order F2003-018*).

Some factors that should be taken into account when exercising discretion include:

- the general purposes of the Act (i.e. public bodies should make information available to the public, and individuals should have access to personal information about themselves);
- the wording of the discretionary exception and the interests which the exception attempts to protect or balance;
- whether the applicant's request may be satisfied by severing the record and providing the applicant with as much information as is reasonably practicable;
- the historical practice of the public body with respect to the release of similar types of records;
- the nature of the record and the extent to which the record is significant or sensitive to the public body;
- whether the disclosure of the information will increase public confidence in the operation of the public body;
- the age of the record;
- whether there is a definite and compelling need to release the record; and
- whether Commissioner's Orders have ruled that similar types of records or information should or should not be disclosed.

(See *IPC Order 96-017*.)



**A public body must not replace the exercise of discretion under Part 1 of the Act with a blanket policy that certain types of information will not be released. Public bodies can develop guidelines to assist in the exercise of discretion, provided they are not interpreted as binding rules. Whether an exception is mandatory or discretionary, the public body must consider whether section 32 of the Act (disclosure in the public interest) requires release of the information.**

### Harms test

Some exceptions (both mandatory and discretionary) are based on a harms test. This generally provides that access to all or part of a record may or must be refused if disclosure could reasonably be expected to harm a particular public or private interest. The general test for harm under the Act is whether there is a reasonable expectation of harm flowing from disclosure of the specific information at issue (see *IPC Order 2000-006*).

*IPC Order 96-003* established a specific test for harm under **section 20**. This test has been applied to other provisions of the *FOIP Act* that refer to harm, such as **sections 16, 18, 21 and 25**. Under this three-part test,

- there must be a reasonable expectation of probable harm;
- the harm must constitute damage or detriment, and not mere inconvenience; and
- there must be a causal connection between disclosure and the anticipated harm.

The evidence must demonstrate a probability of harm from disclosure and not just a well-intentioned but unjustifiably cautious approach to the avoidance of any risk whatsoever because of the sensitivity of the matters at issue. The likelihood of harm must be genuine and conceivable.

The harm must pass a general threshold of damage or detriment, not mere interference or hindrance. The threshold may vary depending on the nature of the harm that may result from disclosure. The harm must be specific to the context of the request. For example, there must be evidence of a direct and specific threat to an individual or a specific harm flowing from the disclosure of the information or record in order to apply **section 18** (harm to health or safety) to withhold records or information from an applicant.

For a detailed discussion of the concept of harm, see IPC FOIP Practice Note 1: *Applying "Harms" Tests*.

### Other tests

A public body can refuse to disclose information if the disclosure would *reveal* information that belongs to a certain class, such as advice from officials, Cabinet confidences, or the substance of deliberations of *in camera* meetings. In such cases there is no need to address the harm that the disclosure may cause, although this may be a factor in exercising discretion.

### Application of exceptions

There is a general process that should be followed in applying all exceptions. There are five basic steps.

#### **Step 1: Preliminary examination**

Meet with public body staff to understand the content of the record(s) and the context and significance of the record(s) at the time they were created and at the time of the request. Undertake a general review of the record(s) to determine which exceptions

may apply and to gauge the complexity of the case and the notices that will be required as part of the process.

**Step 2: Detailed review**

Review the record(s) line by line to consider more thoroughly the nature and extent of the exceptions involved. Identify information that may be subject to mandatory exceptions where a public body has no discretion to disclose information, and information to which no exception applies. Serve any required notices.

**Step 3: Exercise of discretion**

Where discretion is permitted, undertake any necessary consultation and decide, with respect to information where exceptions apply, whether any or all of the information will be withheld.

Multiple discretionary exceptions may be applied to the same record, where there is sufficient justification for doing so.

**Step 4: Severing**

Sever that part of the record(s) to which the public body has decided that it is necessary to refuse access. This will leave a record with a number of blank spaces annotated with references to the section(s) of the Act applied to sever the record. If a sequence of pages has been severed completely, a public body should not disclose a number of blank pages. Instead it may disclose a single page listing the records and the exceptions applied in each case.

**Step 5: Response to applicant**

Prepare a response to the applicant following the guidelines provided in Chapter 3. Many exceptions require careful consideration. Reference should be made to the detailed advice provided in this chapter on the application of each of the specific exceptions.

The processes associated with these steps are discussed in Chapter 3.

**Claiming additional exceptions**

A public body may claim additional exceptions to disclosure after providing a response to an applicant as long as the applicant is notified of the exceptions with enough time to make representations during an inquiry (see *IPC Order 99-033*). The Commissioner will not allow the late application of an exception if this would allow the public body to make a broad after-the-fact justification for its original exercise of discretion to withhold information (see *IPC Order 2000-023*).

**Time limitation on the application of certain exceptions**

Some exception provisions state that the exception does not apply to information in a record that has been in existence for longer than a stated period of time. The exceptions that include a time limitation are **section 16** (third party business information in the archives of a public body), **section 17(2)(i)** (personal information of individual deceased for more than 25 years), **section 20** (harm to law

enforcement), **section 21** (harm to intergovernmental relations), **section 22** (Cabinet confidences), **section 23** (local public body confidences) **section 24(1)** (advice from officials) and **section 24(2.1)** (records of an audit by the Chief Internal Auditor of Alberta).

To determine whether a time limitation applies to a record or information, the public body would compare the number of years stated in the limitation provision with the day and month on the face of the record. For example, **section 21(4)** states that **section 21** does not apply to information that has been in existence in a record for 15 years or more. Therefore, at least 15 years must have elapsed since the record was created.

Where the date the record was created is not obvious, the public body would have to examine the context of the record, other documents that may be in proximity to the record in a file or which may refer to the record and other facts that may help provide a date. Information in a record that fits within an exception under the Act but which is older than the stated time limitation in the exception must be disclosed unless another exception applies to it.

#### 4.2 Disclosure Harmful to Business Interests of a Third Party

**Section 16(1)** creates a mandatory exception for information which, if disclosed, would reveal certain types of third party business information supplied in confidence, and could also result in one or more specified harms.

**Section 16(1)(a) to (c)** provides a three-part test. The information in question must

- be of a type set out in **section 16(1)(a)**;
- be supplied explicitly or implicitly in confidence by the third party (**section 16(1)(b)**); and
- meet one of the harms or other conditions set out in **section 16(1)(c)**.

#### Type of information

**Section 16(1)(a)** This provision states that the head of a public body must refuse to disclose information that would reveal

- a trade secret; or
- commercial, financial, labour relations, scientific or technical information of a third party (**section 16(1)(a)**).

When interpreting **section 16(1)(a)**, the following definitions should be kept in mind:

Third party business information is *explicitly* revealed if the information disclosed is itself third party business information or if it makes direct reference to third party business information.

Third party business information is *implicitly* revealed if the information disclosed allows a reader to draw an accurate inference about third party business information (see *IPC Orders 96-013* and *98-013*).



**Section 16(1)(a)** cannot be applied to information that has already been disclosed, such as information in a part of a proposal that has been disclosed, or information that is not proprietary information of the third party. (See also *IPC Order F2002-002*.)

In deciding whether information in a record falls within **section 16(1)(a)**, the Information and Privacy Commissioner will not rely on the title, but on the content of the record (*IPC Orders 96-013 and 2000-017*), taking into consideration the nature of the information and context in which it appears (*IPC Orders 98-006 and 2001-008*).

**Section 1(s)** *Trade secret* is defined in **section 1(s)** of the Act as information, including a formula, pattern, compilation, program, device, product, method, technique or process,

- that is used, or may be used, in business or for any commercial purpose;
- that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use;
- that is the subject of reasonable efforts to prevent it from becoming generally known; and
- the disclosure of which would result in significant harm or undue financial loss or gain.

Information must meet all of these criteria to be considered a trade secret. The fact that others may benefit from the disclosure of the information does not mean that there is independent economic value in the secrecy of the information (*IPC Order F2004-006*).

Information that is generally available through public sources (e.g. corporate annual reports) would not usually qualify as a trade secret under the Act. A third party must be able to prove ownership or a proprietary interest in a trade secret or must be able to prove a claim of legal right to the information (e.g. a licence agreement) in order for that information to qualify for the exception.

**Section 1(r)** A *third party* is defined in **section 1(r)** of the Act as any person, group of persons or organization other than the applicant (i.e. the person making an access request) or a public body. A third party may be an individual, sole proprietorship, partnership, corporation, unincorporated association or organization, non-profit group, trade union, syndicate, or trust. For example, a contractor providing catering and support services to a public body was found to be a third party to an access request for the contractor's proprietary information (see *IPC Order 99-008*).

Even if one of the members of a partnership is a public body, the partnership may still be a third party under the *FOIP Act* (see *IPC Order 2000-005*).

Employees may also be third parties in certain situations. Individuals interviewed during an investigation related to an employee's misconduct and termination were found to be third parties with respect to their personal information (see *IPC Order 98-008*).

*Commercial information* includes the contract price as well as information that relates to the buying, selling or exchange of merchandise or services (see *IPC Order 96-013*). Commercial information may also include a third party's associations, history,



references, bonding and insurance policies (see *IPC Orders 97-013 and 2001-021*) as well as pricing structures, market research, business plans, and customer records. The names and titles of key personnel and contract managers is commercial information when the information relates to how the third party proposes to organize its work (*IPC Order F2003-004*).

An agreement between two business entities may contain commercial information (see *IPC Order 2001-019*), but the fact that the records requested by an applicant are agreements between two business entities is not determinative of whether **section 16(1)** applies (*IPC Order 2000-017*).

Where a contract contains some third party commercial or financial information, it does not necessarily follow that the entire contract can automatically be withheld under **section 16**. Each provision of a contract must be examined to determine whether it contains, or would reveal, proprietary information that was supplied in confidence to a public body (*IPC Order F2008-019*). At the same time, records need to be viewed as a whole to determine they have the aggregate effect of revealing commercial information (*IPC Orders 98-006 and F2003-004*).

A business letterhead is not commercial information (*IPC Order 98-006*). A business's GST number may be commercial or financial information (*IPC Order F2008-019*).

*Financial information* is information regarding the monetary resources of a third party, such as the third party's financial capabilities, and assets and liabilities, past or present (see *IPC Orders 96-018 and 2001-008*). Common examples are financial forecasts, investment strategies, budgets, and profit and loss statements.

*Labour relations information* relates to the management of personnel by a person or organization, whether or not the personnel are organized into bargaining units. Labour relations information includes relationships between workers, working groups and their organizations as well as managers, employers and their organizations (see *IPC Order 2000-003*). Labour relations information also includes relationships within groups and organizations and collective relations between a public body and its employees.

A dispute between a school board and a school council is not a labour relations dispute, since school council members are not employees of a school board (*IPC Order 2001-010*). A post-secondary institution's internal complaint process for employee disputes about employment obligations is a labour relations dispute-resolution process (*IPC Order F2003-009*).

Common examples of labour relations information are hourly wage rates, personnel contracts and information on negotiations regarding collective agreements.

*Scientific information* is information exhibiting the principles or methods of science (*IPC Order 2000-017*). Applying this definition, the Commissioner decided that operating manuals forming part of a photo radar contract between a public body and a third party contained scientific and technical information (*IPC Order 2000-017*).

*Technical information* is information relating to a particular subject, craft or technique (*IPC Order 2000-017*). Examples are system design specifications and plans for an engineering project.

### **Supplied in confidence**

**Section 16(1)(b)** *Section 16(1)(b)* covers information provided voluntarily by a third party and information provided by a third party under law or some other form of compulsion.

The information would normally have to be supplied by a third party and not compiled by the public body. For example, a report created by an inspector visiting a plant would not qualify as being supplied by the third party. **Section 16(1)(b)** does not cover information that is generated jointly through negotiation with the public body (see *IPC Order 96-013*). However, there may be exceptions where the information supplied to the public body during negotiations remains relatively unchanged in an agreement or could be inferred from an agreement (see *IPC Order 2000-005*).

A letter created by a public body might contain information that would qualify for this exception if it reproduces or analyzes information supplied by a third party in such a way as to reveal the information itself (see *IPC Order 99-007*). In *IPC Order 99-040*, although some of the information withheld consisted of analyses created by the public body and had not been supplied directly by a third party, the information was inextricably linked with information supplied by the third parties, so the confidentiality provision applied.

Financial or commercial information will also be seen as supplied by a third party in confidence if it is originally supplied to a public body in confidence and that public body then supplies the information in confidence to a second public body (see *IPC Order 2001-008*).

The fact that a public body may have released third party information that was intended to have been kept confidential does not limit the third party's ability to claim that the information was supplied in confidence (see *IPC Orders 96-013* and *99-017*).

*In confidence* usually describes a situation of mutual trust in which private matters are related or reported.

*Implicitly*, in the context of **section 16(1)(b)**, means that both parties understand that the information is being supplied in confidence. There may be no actual statement of confidentiality, no written agreement or other physical evidence of the understanding that the information will be kept confidential. In such cases, all relevant facts and circumstances need to be examined to determine whether or not there was an understanding of confidentiality. Some of the relevant facts and circumstances would be how the information was provided, the purpose for which the information was provided, and how the information was managed, secured or distributed by or within the public body.

*Explicitly*, in the context of **section 16(1)(b)**, means that the request for confidentiality has been clearly expressed, distinctly stated or made definite.

There may be documentary evidence that shows that the information was supplied on the understanding that it would be kept confidential. However, it is also acceptable for a statement of confidentiality to be given orally. For the purposes of an inquiry, the person who gave the statement and the person to whom it was made may both offer evidence that the statement was made at the time the information was given.

In *IPC Order 99-018*, the Commissioner established a test for confidentiality that has been cited in many subsequent Orders. He stated that a third party must, from an objective point of view, have a reasonable expectation of confidentiality with respect to the information that was supplied. Furthermore, it is necessary to consider all the circumstances of the case, including whether the information was

- communicated to the public body on the basis that it was confidential and that it was to be kept confidential;
- treated consistently in a manner that indicates a concern for its protection from disclosure by the third party prior to being communicated to the public body;
- not otherwise disclosed or available from sources to which the public has access; or
- prepared for a purpose which would not entail disclosure.

In *IPC Order 2001-019*, the Commissioner agreed that a third party had supplied information in confidence on the evidence that City Council passed a motion acknowledging that a memorandum of understanding was confidential, the document contained a confidentiality clause, the memorandum was negotiated in confidence and confidentiality had been maintained. The Commissioner has recommended that public bodies and private service providers contracting with public bodies ensure that their contracts state whether the parties intend the transaction to be confidential (see *IPC Order 2000-009*).

In *IPC Order 2000-010*, the Commissioner did not find sufficient evidence that a consultant had supplied information in confidence. The confidentiality clause in the contracts required the consultant to treat information received by him as confidential. The clause did not require the public body to treat the information supplied by the consultant as confidential.

In *IPC Order F2003-018*, the Commissioner disagreed with the claim that a report on health and safety audits performed by the applicant was intended to be confidential. There was no sworn or documentary evidence to support the argument that the report was supplied on an implicitly confidential basis. Rather, the evidence indicated that the independent review was part of a cooperative and collaborative dispute resolution process with the applicant.

A boilerplate confidentiality clause on a fax cover sheet is not an indicator that information in the record is supplied in confidence (see *IPC Orders F2004-021* and *F2005-011*).

*Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta, recommends that bidders be encouraged to identify any parts of their submissions that are provided in confidence. If the disclosure of certain information

would be harmful to the business interests of prospective contractors, this should be noted in the document itself or in a covering letter.



**It is not sufficient simply to accept a third party's stamp that documents are confidential or an assertion in third party representations that information was supplied in confidence. There must be evidence to support the assertion or marking and to prove that the information has been treated consistently in a confidential manner. (See IPC Order F2008-019.)**

As part of their ongoing business, public bodies should regularly review their understandings with third parties concerning the provision of information in confidence.

#### **Effect on business interests**

**Section 16(1)(c)** In applying **section 16(1)(c)**, there must be objective grounds for believing that one of the results listed below will occur as a consequence of disclosing the information. It must be shown that disclosure of the information would

- significantly harm the third party's competitive position;
- interfere significantly with the third party's negotiating position;
- result in similar information no longer being supplied to the public body;
- result in undue financial loss or gain to any person or organization; or
- reveal information concerning the resolution of a labour relations dispute.

#### **Harm significantly the competitive position of a third party**

**Section 16(1)(c)(i)** *Harm significantly* in this provision means that disclosure of the information will damage or cause detriment to the third party's competitive position and that the damage or detriment will have considerable impact on the third party.

In order to assess the significance of the harm, a public body should review, among other things

- the nature of the information;
- the third party's representations regarding the harm involved;
- an objective appraisal of that harm, including any monetary or other value placed on it, if this can be determined; and
- the impact on the third party and its ability to withstand this.

Applying the harms test set out in *IPC Order 96-003*, a decision to refuse access under this exception should be supported by detailed evidence showing that the expectation of harm is reasonable and the harm is probable. The evidence must show that

- there is a clear cause and effect relationship between the disclosure and the alleged harm;

- the expected harm amounts to damage or detriment and not simply hindrance or minimal interference; and
- the likelihood of harm from disclosure of the specific information is genuine and conceivable, and not merely speculative; it is not sufficient to show that there is a potential for harm simply because the information is sensitive.

In *IPC Order 2001-019*, the Commissioner agreed that the competitive position of the third party would be harmed because the record in question set out the party's strategic position with respect to its dealings with one public body and this was intended to serve as a blueprint for the third party's proposed and ongoing commercial relationships with other similar public bodies.

In *IPC Order F2002-002*, the Commissioner rejected the argument that disclosure of information in a third party's proposal regarding the company's history and general information about its projects and plans would significantly harm the competitive position of the third party.

***Interfere significantly with the negotiating position of a third party***

**Section 16(1)(c)(i)** This provision allows for situations where disclosure of third party information would have a major impact on ongoing or future negotiations. Completed negotiations are not normally subject to the exception unless there is a good probability that the particular strategies will be used in the future and the disclosure of information relating to completed negotiations would reveal these strategies.

Examples of information to which this provision may apply include negotiating positions, options, instructions and pricing criteria, and points used in negotiations. (See *IPC Order 2001-008*.)

***Result in similar information no longer being supplied to the public body***

**Section 16(1)(c)(ii)** This provision allows for situations where the disclosure of a third party's confidential business information is likely to have a negative effect on the ability of the public body to obtain similar information in the future. This provision is applicable only in cases where there is a continuing public interest in the particular information being supplied. If this is the case, a public body can consider whether disclosure would discourage either the particular third party or another third party from voluntarily supplying information to it or other public bodies.

A third party may assert that it will no longer provide information if it may be disclosed under the *FOIP Act*. However, the public body is required to come to a reasonable decision as to whether or not this will be the case. It is unlikely that similar information will no longer be supplied where the third party has a financial or other incentive to continue supplying the information or where it is legally required. (See *IPC Order 96-018*.)

If a public body can order certain records to be supplied to it under an enactment (e.g. the *Occupational Health and Safety Act*), the records cannot be withheld under **section 16(1)(c)(ii)** of the *FOIP Act* (see *IPC Order 2000-014*).

**Section 16(1)(c)(ii)** might be applicable to the supply of pricing information by a group of third parties which serves to effectively regulate pricing of products, or



information on leases and rental values of commercial properties in order to apply market-value assessments across a city.

**Result in undue financial loss or gain to any person or organization**

**Section 16(1)(c)(iii)** For this provision to apply, there must be objective grounds for believing that disclosing the information would result in an undue loss or gain measured in monetary or monetary-equivalent terms (e.g. loss of revenue, loss of corporate reputation or loss of good will).

The undue financial loss or gain may apply to the public body that has custody or control of the information in question, the third party that supplied the information or any other person or organization.

There must be objective grounds for believing that the loss or gain contemplated by this exception would actually result from disclosure. A public body should be prepared to present detailed and convincing evidence of the facts that led to the expectation that the undue financial loss or gain would occur if the information were disclosed. A link is required between the disclosure of specific information and the result that is expected from the disclosure.

For example, in *IPC Order 96-013*, the Commissioner did not find sufficient evidence showing that disclosure of certain clauses in a contract between the public body and third party would affect the legal relations between the parties or that the parties' existing rights would be different after disclosure.

**Reveal labour relations information**

**Section 16(1)(c)(iv)** This provision allows for the non-disclosure of information that would reasonably be expected to *reveal* either of two specific kinds of labour relations information of a third party:

- *information supplied to* an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute; or
- *the report of* an arbitrator, mediator, labour relations officer or person or body appointed to resolve or inquire into a labour relations dispute.

This provision could apply to the information that was supplied to, or the report of, the person inquiring into the dispute. In either of these cases, the information would have been collected, compiled or created by that person in the course of the dispute resolution process.

This provision could also apply to information that would *reveal* information supplied to the person inquiring into the dispute, or contained in the report of that person. This could include information that makes reference to the positions of the parties in an arbitration process, an account of an interview with a mediator or notes for, or a draft of, the report. Other examples include notes relating to deliberations on the report of a labour relations officer, or any other information that would allow a reader to draw an accurate inference about the information supplied to, or in the report of, a person inquiring into a labour relations dispute.

A *report* may consist of a record providing information or opinions, or a formal statement or account of the results of an analysis of information.

The recording of mere observation or a simple statement of fact would not generally be covered by this provision. The provision requires that an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute create the report.

An *arbitrator* is a neutral person chosen by the parties to a dispute to hear their arguments and give judgment between them. The parties may submit themselves voluntarily or under a compulsory agreement to the arbitrator's decision.

A *mediator* is a person who facilitates discussion between parties who disagree, with the aim of reconciling them.

The mediation does not have to be successful for the person appointed to resolve a dispute to be considered a mediator. Even if the record in question is not considered to be the report of a mediator, the report can still be considered to be the report of a person appointed to resolve or inquire into a labour relations dispute under **section 16(1)(c)(iv)**. (See *IPC Order 2000-003*.)

A *labour relations officer* is any person appointed to inquire into or resolve any form of labour relations dispute or issue.

*Other persons or bodies* appointed to resolve or inquire into a labour relations dispute includes any person or body appointed by any level of government or any public body; for example, Cabinet appointments, ministerial appointments, appointments by the council, board or the chief executive officer of a public body.

One example of other persons or bodies appointed to resolve or inquire into a labour relations dispute would be the ministerial appointment of a disputes inquiry board to attempt to resolve a dispute involving a school board. Another example would be the designation by the Director of the Labour Relations Board of a person requested by parties to a dispute as an officer of the Board.

### **Tax information**

**Section 16(2)** This exception provides that a public body must refuse to disclose information about a third party that was collected on a tax return or collected for the purpose of determining tax liability or collecting a tax. This is a mandatory exception. The public body cannot disclose the information unless required to do so by law or by **section 32** (disclosure in the public interest). An example of a required disclosure would be the provision of a tax certificate by municipalities under the authority of the *Municipal Government Act*.

*Information collected on a tax return* is information on a form used to determine taxes to be paid for municipal, education, provincial or federal purposes, and includes corporate, business and personal tax information of a third party (see also section 4.3 of this chapter).

*Collected for the purpose of determining tax liability* means collected for the purpose of determining whether a person or organization owes past, present or future taxes to a school board, a municipality or the provincial or federal government.

*Collected for the purpose of collecting a tax* means collected by authorities for the purpose of collecting due or overdue taxes for a school jurisdiction, municipality or the provincial or federal government.

The type of information to which **section 16(2)** may apply includes tax data derived from tax forms, audits of a business intended to determine whether taxes are owed, and information about directors of a bankrupt corporation gathered to determine who should be liable for taxes that are in arrears.

In *IPC Order 2000-024*, the Commissioner ruled that the exception to disclosure of tax information applied to the names and mailing addresses of property owners on an assessment roll because the information was collected for the purpose of determining property tax liability or for collecting property taxes.

**Section 16(2)** may not be used to withhold an applicant's own tax information, since this is not information about a third party.

**Section 16(2)** may be used in relation to information concerning royalties or obtained in the process of collecting royalties. However, such royalties must have a statutory basis as a tax. Where there is doubt about the nature of a royalty, legal advice should be sought.

#### **When the exception does not apply**

**Section 16(3)** A public body may not withhold information under **section 16(1)** or **(2)** if any of the conditions set out in **section 16(3)** are applicable.

#### ***If the third party consents***

**Section 16(3)(a)** A public body cannot withhold requested information under this exception when the third party concerned has consented to disclosure, although other exceptions may be applied to the information. Consent should be in writing. In order for consent to be valid, it must refer to a specific disclosure.

For example, a public body cannot infer that the third party has consented to the disclosure in response to a FOIP request simply because the third party knew that the public body might be obliged to disclose certain records during hearings of an administrative tribunal (see *IPC Order 2001-021*). Also, the acceptance of the terms and conditions of an Request For Proposal process, including the Minister's right to publish summary cost information, does not constitute consent under **section 16(3)** (see *IPC Order F2002-002*).

If the third party neither consents nor objects to the disclosure, the public body must assess the appropriate application of this exception. It always remains the responsibility of the public body to make the final decision, taking into consideration all relevant circumstances.

A third party may consent to the disclosure of some but not all of the information in which the third party has a business interest.

For further discussion of consent see Chapter 5 which deals with third party notices, and FOIP Bulletin No. 10: *Third Party Notice*, published by Access and Privacy, Service Alberta.

***If an enactment of Alberta or Canada authorizes or requires disclosure***

**Section 16(3)(b)** The information must be disclosed where disclosure is provided for in other provincial legislation or in federal legislation. For example, the *Environmental Protection and Enhancement Act* lists information that the Department of Environment must, or is authorized to, disclose to the public (see *IPC Order F2005-030*).

***If the information relates to a non-arm's length transaction between a public body and another party***

**Section 16(3)(c)** This provision, which is intended to make transactions between public bodies and other parties more transparent, applies in circumstances where a public body is a direct participant in a transaction and is working with the other party.

**Section 16(3)(c)** applies to provincial government public bodies and local public bodies.

The definition of a non-arm's length transaction in **section 4(4)** of the Act is not applicable to this section. In this case, a *non-arm's length transaction* is a transaction in which one of the parties may be influenced in its bargaining by something other than individual self-interest, or one of the parties may have sufficient leverage or influence to exercise control or pressure on the free will of the other (see *IPC Order 98-013*).

An example would be an agreement between a corporation and the Government of Alberta to invest in and pursue a project together.

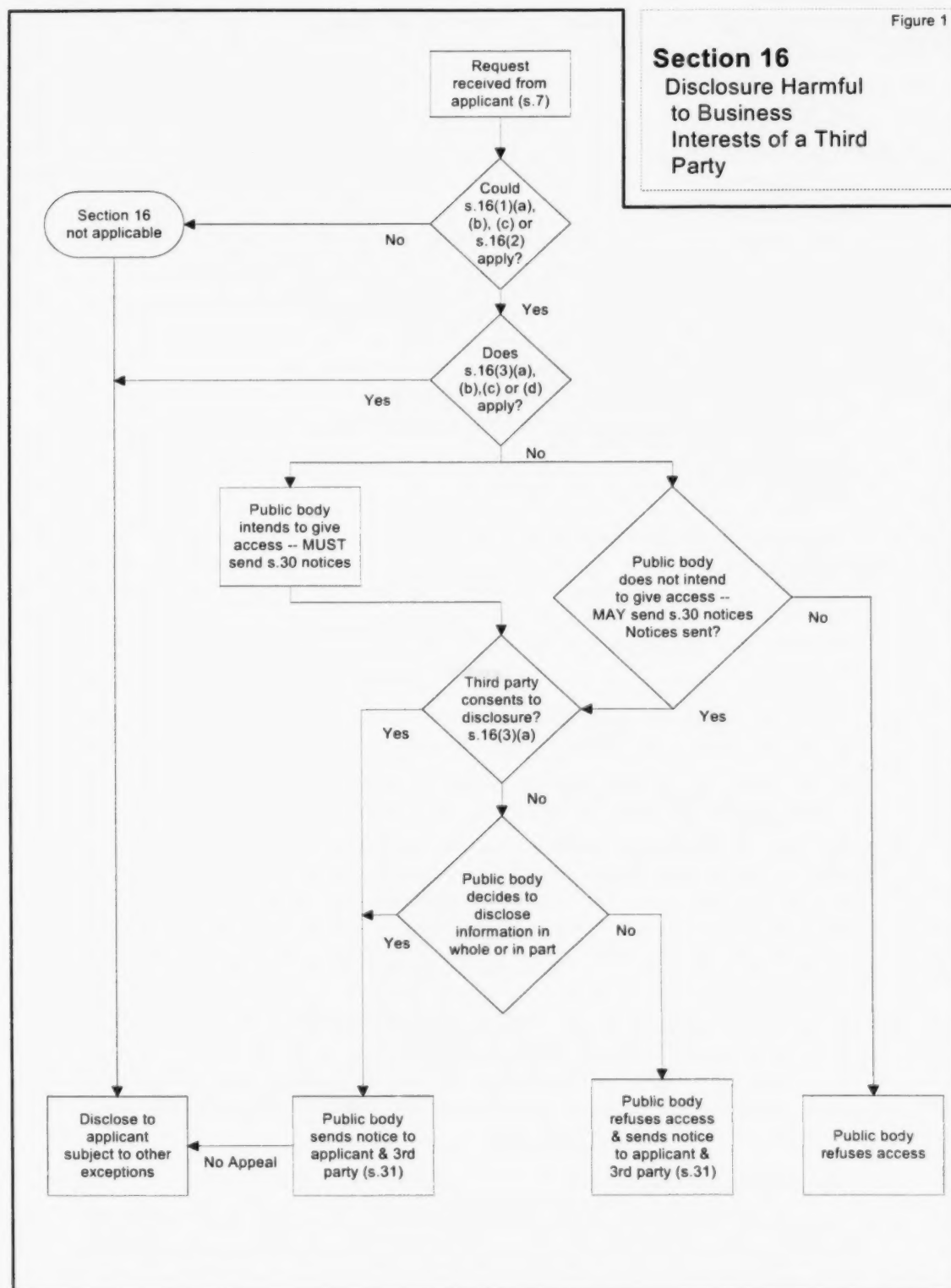
***If the information is in a record in the archives of a public body and has been in existence for 50 years or more***

**Section 16(3)(d)** This provision recognizes that the sensitivity of business information decreases with time, and so does the injury that might occur to the business interests of a third party as a result of disclosure. The fact that such information resides in the Provincial Archives or in the archives of a public body means that the information is considered of historical value. The Act therefore makes it available for research after the passage of 50 years.

Disclosure of third party business information from the Provincial Archives or the archives of a public body can take place earlier, that is, after 25 years from the date of the record, if the disclosure would not be harmful to the business interests of a third party. See **section 43(1)(b)(i)** and section 10 of Chapter 7 for a further discussion on disclosure of information in archives.

**Application of exception**

A number of steps are involved in considering whether or not information qualifies for an exception to disclosure under **section 16**. These steps are set out in Figure 1.





### 4.3 Disclosure Harmful to Personal Privacy

**Section 17** of the Act protects the privacy of individuals whose personal information may be contained within records responsive to a FOIP request made by someone else. In the exception, the individual the information is about is referred to as a *third party*. Third party personal information must not be disclosed when this would constitute an unreasonable invasion of the third party's privacy.

The exception applies only to identifiable individuals and not to groups, organizations or corporations (*IPC Order F2003-004*). Employees of a company contracted by a public body are third parties (*IPC Order F2004-024*).



**Whenever a request for records includes third party personal information, as defined in section 1(n) of the Act, the public body must determine whether disclosure would be an unreasonable invasion of the third party's personal privacy.**

#### Definition of personal information

A detailed explanation of the definition of personal information in **section 1(n)** is provided in section 1.3 of Chapter 1. The examples given are non-exhaustive and do not define personal information in its entirety. Other examples include photographic images, e-mail addresses and an individual's membership in business, professional or benevolent organizations or labour unions.

To qualify as personal information under the Act, information must be written, photographed, recorded, or stored in some manner. However, for the purposes of **Part 2** of the Act, disclosure of previously recorded personal information can include oral transmission by telephone or in person. The individual may be named in the record or it may be possible to ascertain or deduce the identity of the individual from the contents of the record. Public bodies need to consider the context of a record to determine whether an individual may be identifiable to an applicant who may or may not be aware of a given set of circumstances.

The Information and Privacy Commissioner has decided that information related to a sole proprietorship is not personal information (*IPC Order F2002-006*).

#### Exception for personal information

*Section 17(1)* **Section 17(1)** establishes a mandatory exception to disclosure for personal information if the disclosure would be an unreasonable invasion of a third party's personal privacy. When this is the case, the public body must refuse to release the information.

#### Disclosure not an unreasonable invasion of a third party's privacy

*Section 17(2)* **Section 17(2)** sets out those circumstances where disclosure of personal information is *not* considered to be an unreasonable invasion of a third party's personal privacy.

In these circumstances, a public body may not rely on **section 17** to refuse disclosure of personal information. However, other sections of the Act should still be considered when making a decision about disclosure.

**Section 17(2)** states that disclosure of personal information is not an unreasonable invasion of an individual's personal privacy if

- the third party has, in the prescribed manner, consented to or requested the disclosure;
- there are compelling circumstances affecting anyone's health or safety, and written notice of the disclosure is given to the third party;
- an Act of Alberta or Canada authorizes or requires the disclosure;
- the information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a public body;
- the disclosure reveals financial and other details of a contract to supply goods or services to a public body;
- the disclosure reveals the nature of a licence, permit or other similar discretionary benefit that has been granted to a third party by a public body and relates to either a commercial or professional activity or to real property;
- the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body;
- the personal information is about an individual who has been dead for 25 years or more; or
- the disclosure is not contrary to the public interest and reveals only the following information about a third party:
  - enrolment in a school of an educational body or in a program offered by a post-secondary educational body,
  - attendance at or participation in a public event or activity related to a public body, including a graduation ceremony, sporting event, cultural program or club, or field trip, or
  - receipt of an honour or award granted by or through a public body.

The provisions of **section 17(2)** are discussed in more detail below.

#### **Consent to or request for disclosure**

**Section 17(2)(a)** The exception to disclosure does not apply where the individual either consents to or requests the disclosure. This consent or request must be in the prescribed manner and must be specific. Consent in such circumstances normally comes after third party consultation. Implied consent is not sufficient to satisfy this condition.

The requirements for valid consent are set out in **section 7** of the FOIP Regulation. **Section 7** allows for consent to be in writing, in electronic form or given orally.

When a public body consults with a third party and the third party consents to the disclosure of his or her personal information, the information cannot be withheld under **section 17**. However, the public body should review the other exceptions to disclosure in the Act to see whether the information may or must be withheld under one of those exceptions (see *IPC Order 2000-029*).

A public body may decide not to disclose a third party's personal information without consulting with the third party. If the applicant requests a review by the Information

and Privacy Commissioner, the Commissioner may issue a notice to the third party at that time (**section 67(1)(a)(ii)** of the *FOIP Act*).

Consent can be provided to the public body on behalf of the individual by certain persons and under certain conditions as set out in **section 84** of the Act. The exercise of rights by others is discussed in detail in section 2.5 of Chapter 2.

**Compelling circumstances affecting anyone's health or safety**

**Section 17(2)(b)** This provision applies only when there are compelling circumstances affecting the health or safety of any person. To rely on this provision a public body must be able to show that disclosure of the information requested is likely to have a direct bearing on the compelling health or safety matter (see *IPC Orders 97-002, 98-007 and 2001-001*).

Depending upon the urgency of the compelling circumstances, it may be necessary to consider disclosing third party personal information in the public interest under **section 32** prior to the time that a response to a request is due under **Part 1** of the Act.

In applying **section 17(2)(b)**, the public body is required to give written notice of disclosure to the third party whose personal information the public body is disclosing. **Model Letter R** in Appendix 3 may be used in these situations. See **section 83** and section 2.6 of Chapter 2 regarding the manner of giving notices.

**Act of Alberta or Canada authorizes or requires disclosure**

**Section 17(2)(c)** It is not an unreasonable invasion of personal privacy to disclose personal information if disclosure is authorized or required by a provincial or federal statute. In applying the exception, a public body must first consider whether the section of the other statute specifically applies to certain information in the record and then only disclose that part of the record containing the relevant information.

**Classification, salary range, discretionary benefits or employment responsibilities of public officials**

**Section 17(2)(e)** The disclosure of certain employment information about officers, employees or members of public bodies is not an unreasonable invasion of personal privacy. The rationale is that more information should be available about individuals who are paid out of public funds (see *IPC Order F2004-014*).

**Section 17(2)(e)** applies to employer–employee (contract of service) relationships, as opposed to fee-for-services or independent contractor (contract for service) relationships, which fall within **section 17(2)(f)** (*IPC Order F2004-014*). Classifications, salary ranges and discretionary benefits are characteristic of an employer–employee relationship, whereas fixed duration and fixed price or fixed number of hours to be worked are typical of a fee-for-services contract.

*Classify* means to assign (a thing) to a class or category (*IPC Order F2005-016*).

*Employee* is defined in **section 1(e)** of the Act as including a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with a public body.

*Volunteer* means a person who voluntarily takes part in an enterprise or offers to undertake a task and a person who works for an organization voluntarily and without pay. *Voluntary* means done, acting or able to act of one's free will; not constrained or compulsory, intentional; unpaid (IPC Order F2002-006).

The definition of "employee" includes all individuals appointed to boards or committees, individuals providing voluntary services on behalf of a public body, students who volunteer or are participating in a work-experience program and individuals employed under a personal service contract. For example, a person that undertook to review certain audits was considered a volunteer, and therefore an "employee" of the public body, for the purposes of the Act (IPC Order F2002-006).

**Employment responsibilities.** Section 17(2)(e) establishes that the disclosure of information about an employee's actual job classification and responsibilities is not an unreasonable invasion of an individual's personal privacy.

*Employment responsibilities* encompasses those duties than an individual is charged with performing as an officer, employee or member of a public body (IPC Order F2005-016).

A job title or position is information about employment responsibilities (IPC Order F2003-002).

A description of an employee's employment responsibilities, which is personal information, is to be distinguished from information that records the employee's execution of his or her duties. What an employee has done in his or her professional or official capacity is not personal information, unless the information is evaluative or is otherwise of a "human resources" nature, or there is some other factor which gives it a personal dimension (i.e. makes the information "about" the individual) (IPC Orders F2004-026, F2006-030, F2007-029 and F2008-019).

**Section 17(2)(e)** does not permit the disclosure of information about an employee's performance or conduct, such as an annual performance evaluation or an investigation into an employee's conduct (IPC Order 97-002).

**Salary range.** Under section 17(2)(e), it is not an unreasonable invasion of personal privacy to disclose the salary range for an employment position.

*Salary* means a fixed regular payment made by an employer to an employee (IPC Order F2004-014).

*Range* means a series representing variety or choice; a selection (IPC Order F2005-016).

An actual salary is not a salary range and therefore cannot be disclosed under **section 17(2)(e)** (IPC Order F2005-016). An exact salary may nevertheless be disclosed where, upon consideration of all relevant factors (**section 17(5)**), it is determined that the disclosure would not be an unreasonable invasion of the third party's privacy (see IPC Orders F2006-007, F2006-008 and F2008-010).



Where no salary range exists, a public body should consider creating one in order to support disclosure of information that promotes accountability for the expenditure of public funds.

A salary increment that is based on an assessment of the employee's performance is not information about the employee's salary or a salary range, nor is it a discretionary benefit. The increment is an evaluation and its disclosure is presumed to be an unreasonable invasion of personal privacy under **section 17(4)(f)** (*IPC Order F2007-015*).

**Discretionary benefits.** **Section 17(2)(e)** establishes that the disclosure of a discretionary benefit provided on an individual basis, rather than in accordance with a plan, scale or formula, including any allowance with monetary value that the public body chooses to provide, is not an unreasonable invasion of an individual's privacy.

(See the discussion under **section 17(2)(g)** for the meaning of the words "benefit" and "discretionary.")

**Section 17(2)(e)** is intended to capture a range of discretionary benefits that flow from the employment relationship (*IPC Order 2001-020*). The provision requires the discretionary benefit to be received by the third party in his or her capacity as an officer, employee, or member of a public body. Therefore, **section 17(2)(e)** did not apply to the discretionary benefits in a settlement agreement that were being provided to the third party in his capacity as a *former* employee (*IPC Order F2007-025*).

**Section 17(2)(e)**, unlike **section 17(2)(h)**, does not require the benefit to be provided by a public body; the benefit may be provided by another entity (*IPC Order F2007-025*).

In *IPC Order F2003-002*, it was decided that it was not an unreasonable invasion of a personal privacy to disclose the supplementary pension formula and clauses relating to the administration of the pension benefits in a severance agreement. The portions of the severance agreement that could be disclosed were discretionary benefits because the City had a choice as to whether it would grant the benefits. The City was ordered to withhold the name, retirement date and signature of each pension recipient. (See also *IPC Orders 98-014* and *98-018*.)

In *IPC Order 2001-020*, a severance package was considered to be an employment-related discretionary benefit for the purposes of **section 17(2)(e)**. The Information and Privacy Commissioner held that the severance package in that case was a beneficial payment or advantage that flowed from the employment relationship to the employee whether it was actually paid before the relationship formally ended and whether it was required by law.

In *IPC Order F2006-007*, the amount of vacation time and pay, termination notice and pay, disability insurance benefits and pension plan benefits of a senior official were discretionary benefits flowing from the employment relationship (see also *IPC Orders F2006-008* and *F2007-025*).



**Contracts to supply goods and services to a public body**

**Section 17(2)(f)** The disclosure of financial and other details about the supply of goods and services to a public body is not an unreasonable invasion of privacy, even when these details may be personal information (see *IPC Order F2004-014*). The rationale is that the public is entitled to know from whom and for what amount such services were purchased (see *IPC Order F2004-024*). This is an important part of public accountability.

*Financial details* relates to the amounts paid under the contract.

*Other details* include the names of the parties, the subject of the contract and standard boilerplate terms and conditions. Other details would not include résumés of employees of contractors that may be attached as an appendix to the contract.

*Contract to supply goods and services* refers to an agreement concluded by a public body with a third party to buy or sell products, merchandise, or services, as well as to an agreement entered into by a public body in relation to employment or performance of work-related duties. It does not apply where a public body provides money to a third party to provide contracted services to a party other than a public body (see *IPC Order 98-004*).

Whether an employment contract falls under **section 17(2)(f)** or **section 17(2)(e)** will depend on the terms of the contract and the nature of the relationship between the public body and the third party (*IPC Order F2008-010*). **Section 17(2)(f)** applies to fee-for-services or independent contractor (contract *for* service) relationships whereas **section 17(2)(e)** applies to employer–employee (contract *of* service) relationships (*IPC Order F2004-014*).

In releasing this type of information, public bodies should ensure that they are not disclosing information that may be subject to **section 16**, a mandatory exception for disclosure of information which would be harmful to third party business interests.

**Licence, permit or similar discretionary benefit relating to a commercial or professional activity or to real property**

**Section 17(2)(g)** The disclosure of information about discretionary benefits granted by a public body to a third party is not an unreasonable invasion of personal privacy. The intent of this provision is to ensure accountability on the part of public bodies with respect to monetary and other benefits that fall within its discretion. Disclosure under this provision is limited to licences, permits or other discretionary benefits relating to a commercial or professional activity, or to real property.

*Licence or permit* means authorization to carry out an activity, such as operating a particular establishment, or carrying on a professional or commercial activity.

*Commercial activity* means an activity that relates to the buying, selling or exchange of merchandise or services.

Examples of licences or permits that fall within this provision include business licences, teaching permits, taxi licences, and building and development permits.

Licences or permits for commercial activity do not include licences or permits for solely recreational activities (*IPC Order F2002-011*).

*Benefit* means a favourable or helpful factor or circumstance, or an advantage. For example, a grazing lease on public land falls within the definition of benefit (*IPC Order 98-014*).

*Other similar discretionary benefit* in **section 17(2)(g)** implies that the licence or permit must also have the character of a discretionary benefit (*IPC Order 98-018*).

*Discretionary* refers to the power of a decision-maker to determine whether, or how, to exercise a power or grant a benefit.

In *IPC Order 98-018*, it was decided the granting of grizzly bear hunting licences was not discretionary. The licences were granted as a result of a random draw, not on the basis of applying a set of criteria.

The power to suspend, cancel or reinstate a licence or permit is an indication that the licence or permit is a discretionary benefit. So too is the power to limit or allocate permits by setting formulae or limiting numbers (see *IPC Orders 98-014* and *98-018*).

In *IPC Order F2002-011*, the Commissioner found that an “allocation” granted to an outfitter-guide was a permit that had the characteristics of being a discretionary benefit. A transfer, including a lease, of an allocation was not a licence or permit but was a similar discretionary benefit. It was determined that information about the nature of an allocation included information on the number of allocations held by an individual, the area, species, and manner of hunting, the acquisition, transfer and reversion of allocations, and the renewal and transfer fees. Under **section 17(2)(g)**, this information could be disclosed.



Disclosure under this provision must be limited to the name of the person to whom the licence, permit or discretionary benefit is provided, and the nature of the benefit. It must not include personal information supplied in support of the application for the benefit (see *IPC Investigation Report F2002-IR-006*).

### ***Discretionary benefit of a financial nature***

**Section 17(2)(h)** This provision enables disclosure of information that reveals details of a discretionary financial benefit granted to an individual by a public body.

*A discretionary benefit of a financial nature* is any monetary allowance that the public body may decide to provide (e.g. a scholarship or a grant).

*Grant* means to “give” or “confer” discretionary benefits in situations where there is no requirement by the grantor to provide such benefits (*IPC Order F2007-025*).

*Details* of a financial discretionary benefit are not limited to the amount paid to the third party, but include the third party’s name, the reasons for providing the benefit and any consideration given to the public body in exchange for granting the benefit.

**Section 17(2)(h)** does not apply to information regarding eligibility for income assistance or social benefits, or regarding the determination of individual benefit levels since these benefits are discretionary; they are calculated according to entitlement formulae.

Also, **section 17(2)(h)** does not apply to discretionary benefits that are received by a third party in his or her capacity as an officer, employee or member of a public body since these benefits are covered by **section 17(2)(e)**. **Section 17(2)(h)** does apply to discretionary benefits in a settlement agreement reached with a public body where the benefits are being provided to the third party in his capacity as a *former* employee (*IPC Order F2007-025*).



**Section 17(2)(h)** does not apply to background personal information required by the public body or provided voluntarily by an individual applying for a benefit.

#### **Individual dead for 25 years or more**

**Section 17(2)(i)** This provision puts a time limit on the protection of privacy after death. The *FOIP Act* protects the personal information of an individual who has been dead less than 25 years, with certain exceptions. Once an individual has been dead 25 years or more, release of his or her personal information is deemed not to be an unreasonable invasion of the individual's privacy. The provision is particularly important for permitting historical and genealogical research.

The onus is on the applicant to produce evidence, such as a death certificate, that an individual has been dead for 25 years or more. For more information on disclosure to a relative of a deceased person, see section 7.7 of Chapter 7. See also FOIP Bulletin No. 16: *Personal Information of Deceased Persons*, published by Access and Privacy, Service Alberta.

#### **Disclosure not contrary to the public interest**

**Section 17(2)(j) and 17(3)** The *FOIP Act* allows a public body to disclose categories of third party personal information specified in **section 17(2)(j)**, without consultation and without consent, if the disclosure is not contrary to the public interest. Under this provision, unless an individual has previously requested non-disclosure of his or her information, a public body could disclose class photos, lists of graduates or names of visitors in the Legislature Gallery, for example. The records may be current or historical.

It is not an unreasonable invasion of a third party's personal privacy to disclose personal information if

- the personal information fits within one of the listed categories of information;
- the disclosure is not contrary to the public interest; and
- the individual the personal information is about has not requested that the information not be disclosed.

*Not contrary to the public interest* in **section 17(2)(j)** may be understood as not inconsistent with long-term community values, or with the good of society at large.

A public body is not required to find that a disclosure *promotes* a public interest simply that disclosure is *not contrary to* the public interest. The test for what is “not contrary to the public interest” is different from the test in **section 32(1)(b)**, which provides for disclosure of information that is *clearly in the public interest*, or **section 93(4)(b)**, which allows a public body to excuse fees where an access request *relates to a matter of public interest*.

When considering a request to which **section 17(2)(j)** may apply, a public body must take into account the circumstances surrounding the request. A public body may decide that a disclosure would be contrary to the public interest on the basis of its knowledge of risks to its clientele or the nature of the request. For example, if the requested information could be used to commit a criminal act or harm an individual or property, then it is likely to be contrary to the public interest to disclose the information.

In *IPC Investigation Report F2002-IR-001*, the Commissioner’s Office said that a public body must take into account the expectations that an ordinary person might have for how his or her privacy will be respected. A school district was found to have contravened **Part 2** of the *FOIP Act* by posting a student’s test results on a school bulletin board without the parents’ consent. The school district could not rely on **section 40(1)(b)** in conjunction with **section 17(2)(j)** to disclose the information. Given the consensus of outside authorities that public disclosure of test results should be avoided, the school district should have contacted the student and his parents prior to disclosing the results.



When determining whether information should be disclosed, public bodies should consider whether any other exception in the Act applies to the information.

**Section 17(2)(j)** and **section 17(3)** provide for the *disclosure* of specified recorded personal information that it was authorized to collect in the first place. A public body cannot rely on these provisions to *collect* personal information.

#### ***Enrolment in a school, or in a program of a post-secondary educational body***

**Section 17(2)(j)(i)** This provision allows a school board, charter school or regional authority (all as defined in the *School Act*) to confirm that an individual is or was enrolled in a school under its jurisdiction. A post-secondary educational body can confirm that an individual is or was enrolled in a specific program at that institution. An educational body may also provide lists or class photographs of the individuals currently or formerly enrolled in a particular school or post-secondary program (e.g. the students in a particular high school or the students in a particular apprenticeship program). This information is often requested to organize school or program reunions.



This provision does not allow disclosure of whether an individual is physically in attendance at a school or post-secondary institution at a particular time. Nor does it allow disclosure of an individual's timetable of studies or other personal information related to his or her educational program, or personal information unrelated to enrolment, such as the individual's home address.

**Attendance at or participation in a public event or public activity**

**Section 17(2)(j)(iii)** This provision allows a public body to disclose a record of the names of individuals who are recorded as having attended or participated in a public event or activity.

*A public event related to a public body* means something of importance that happens or takes place, is of a public nature, and is related to a public body.

*A public activity related to a public body* means a particular occupation or pursuit that is staged in public and is related to a public body.

*Related to a public body* means connected with the public body's mandate and functions and organized or sponsored by the public body.

An event or activity would be considered *public* if it was open to the public in general, or to a section of the public. The event or activity may be completely open and accessible to the public without charge, or access may be restricted because of the nature of the event or activity, for example, through ticket sales.

The fact that an event or activity that took place on the premises of a public body was observable by a member of the public does not make it a public event or activity.

**Section 17(2)(j)(iii)** does not apply to

- events or activities that are organized or sponsored by a third party that rented a facility owned by a public body;
- events that were not authorized or sponsored by a public body; or
- activities of arm's-length bodies such as "Foundations" or "Friends."

**Receipt of an honour or award granted by or through a public body**

**Section 17(2)(j)(iv)** This provision allows the disclosure of information concerning the *receipt* of an honour or award. This means that the individual must have actually received the honour or award. **Section 17(2)(j)(iv)** does not allow disclosure of an offer of, or qualification for, an honour or award if the honour or award was not presented, or if the honour or award was declined. The honour or award must be granted by a public body (e.g. a degree, scholarship, or merit award) or be granted through a public body on behalf of some other institution or person (e.g. a prize or award sponsored by a private-sector organization which is granted by a post-secondary institution on the basis of the recipient's performance in the institution's programs).

A public body can disclose the information that a particular honour or award has been granted to a particular individual and can disclose a list of names of individuals who



have received a particular honour or award. Disclosure of a photograph of an individual named as a recipient of a current or past award would also be allowed, if the photograph was collected for the purpose of the awards program, or if disclosure of another photograph would be consistent with the purpose for which the photograph was collected.

The provision does not allow disclosure of personal information unrelated to the receipt of the award, such as the recipient's educational history.

#### ***Request for non-disclosure of personal information***

**Section 17(3)** **Section 17(3)** allows an individual to request that information described in **section 17(2)(j)** not be disclosed under that provision.



**If a request for non-disclosure is made, it would be an unreasonable invasion of that individual's personal privacy to disclose any of the information that the individual has requested not be disclosed under section 17(2)(j). This may include all or part of the information referred to in section 17(2)(j).**

A public body is not expected to seek an individual's consent to disclose personal information to which **section 17(2)(j)** applies. In addition, the Act's provision for third party consultation does not apply in this situation (**section 30(2)**).

However, a public body is expected to have a process in place for notifying individuals that they have the right under the *FOIP Act* to request non-disclosure so that they can exercise the right if they wish. Notice of this right can be given in the same way and at the same time as information is given about the collection of personal information. The notice may be given orally, on a form, or in a brochure or other publication.

Public bodies must ensure that procedures are in place so that requests for non-disclosure can be honoured and that no inadvertent disclosure of personal information takes place.

For a more detailed discussion of **sections 17(2)(j)** and **17(3)**, see FOIP Bulletin No. 4: *Disclosure of Personal Information "Not Contrary to the Public Interest,"* published by Access and Privacy, Service Alberta.

#### ***Presumption of unreasonable invasion of privacy***

**Section 17(4)** **Section 17(4)** sets out particular types of personal information the disclosure of which is *presumed* to be an unreasonable invasion of a third party's personal privacy. The decision-maker proceeds from the assumption that disclosure would be an unreasonable invasion of personal privacy unless there is sufficient evidence to the contrary. In determining whether disclosure would be an unreasonable invasion of the third party's personal privacy, the head of the public body must consider the factors in **section 17(5)**, as well as any other relevant circumstances.

**Section 17(4)** provides that disclosure of personal information is presumed to be an unreasonable invasion of a third party's privacy if the personal information

- relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;
- is an identifiable part of a law enforcement record, except to the extent that disclosure is necessary to dispose of the law enforcement matter or to continue an investigation;
- relates to eligibility for income assistance or social services benefits or to the determination of benefit levels;
- relates to an individual's employment or educational history;
- was collected on a tax return or gathered for the purpose of collecting a tax;
- consists of an individual's bank account information or credit card information;
- consists of personal recommendations or evaluations, character references or personnel evaluations;
- consists of the third party's name when
  - it appears with other personal information about the third party; or
  - the disclosure of the name itself would reveal personal information about the third party; or
- indicates the third party's racial or ethnic origin, or religious or political beliefs or associations.

These types of personal information tend to be particularly sensitive. In interpreting this provision, the following explanations should be considered.

***Medical, psychiatric or psychological information***

**Section 17(4)(a)** This provision covers records relating to an individual's physical, mental or emotional health, including, for example, diagnostic, treatment and counselling information. Public bodies that are also custodians under the *Health Information Act* need to comply with the access request and disclosure provisions of that Act when dealing with health information.

**Section 17(4)(a)** applies to medical and psychological information appearing in records of disciplinary decisions (*IPC Order F2008-009*). The provision does not apply to fitness requirements for a specialized position (e.g. Chief of Police) (*IPC Order F2005-016*).

***Information that is an identifiable part of a law enforcement record***

**Section 17(4)(b)** This provision applies to individually identifying information in law enforcement records.

*Law enforcement* is defined in **section 1(h)** of the *FOIP Act*. Under this definition, as interpreted by the Commissioner, *law enforcement record* means a record concerning policing or a record concerning a police, security or administrative investigation or proceeding that leads or could lead to a penalty or sanction; in this latter case, the investigation or proceeding must concern the contravention of a statute or regulation that provides for the penalty or sanction (*IPC Orders 2000-019* and *2000-023*). The

definition also includes the complaint that gave rise to a law enforcement investigation.

**Section 17(4)(b)** applies, for example, to records concerning investigations (including the complaints) and proceedings relating to offences under the *Criminal Code* (Canada), offences under other federal and provincial statutes and regulations and contraventions of municipal bylaws, where the applicable statute, regulation or bylaw provides for a penalty or sanction. Examples of a penalty or sanction include imprisonment, a fine, revocation of a licence, or an order requiring a person to cease an activity.

This provision does not apply to administrative investigations that do not involve contraventions of law, such as an investigation into a breach of an employment policy, which may result in disciplinary action. This kind of information is likely to be protected under other provisions of **section 17(4)**.

Disclosure to an applicant of a third party's personal information in a law enforcement record is not presumed to be an unreasonable invasion of privacy if disclosure is necessary to dispose of the law enforcement matter or to continue the investigation. **Section 17(4)(b)** recognizes that a public body that is in possession of evidence relating to a law enforcement matter must have the power to disclose that evidence to the police, another law enforcement agency and to Crown counsel or other persons responsible for prosecuting the offence or imposing a penalty or sanction.

In *IPC Order F2003-005*, **section 17(4)(b)** did not apply to records created during an internal investigation that related to the enforcement of a post-secondary institution's sexual harassment policy rather than a law.

For further information on law enforcement, see FOIP Bulletin No. 7: *Law Enforcement*, published by Access and Privacy, Service Alberta.

**Information that relates to eligibility for income assistance or social service benefits**

**Section 17(4)(c)** This provision relates to monetary benefits provided by municipal, federal or provincial governments to augment an individual's earnings, as well as non-monetary contributions that help supplement earnings from another source. Disclosure of such information is presumed to be an unreasonable invasion of personal privacy.

For personal information to fall under **section 17(4)(c)**, it must relate to eligibility for income assistance or social service benefits or to the determination of benefit levels.

*Relate* means that a connection or association must be established between the personal information and the eligibility or determination (*IPC Order 98-004*).

*Eligibility* means whether a person qualifies to receive income assistance or social service benefits (*IPC Order 98-004*).

### **Employment or educational history**

**Section 17(4)(d)** *Employment history* in **section 17(4)(d)** is a broad, general phrase that covers information pertaining to an individual's work record (*IPC Order 2001-020*).

Employment history is a complete or partial chronology of a person's working life such as might appear in a résumé or personnel file. A written account of a workplace incident or event will not be considered to be part of employment history unless the event or incident is important enough to merit an entry in the personnel file. **Section 17(4)(d)** will apply only to those records that might appear in a personnel file (*IPC Orders F2003-005 and F2004-015*).

Notes made during a workplace investigation were not employment history as they would not normally be included in a personnel file. The results or conclusions of an investigation may be part of a personnel file and therefore be part of a person's employment history (*IPC Orders F2004-015, F2008-014 and F2008-015*).

A record that a formal disciplinary hearing occurred, even if it was discontinued or concluded in favour of the employee, would likely be part of a personnel file and there would be employment history (*IPC Order F2008-009*).

The amount of an individual's salary is not employment history as a salary is not an event and would not form part of a chronology of a person's working life (*IPC Orders F2006-007 and F2008-010*).

An employee number and the year of retirement is employment history (*IPC Order F2004-028*).

The termination date of a current contract is not employment history because the term is still in the future and could not be considered "history" (*IPC Order F2006-008*).



This presumption of unreasonable invasion of privacy does not apply to some employment information about officers, employees and members of public bodies such as position descriptions, salary ranges and discretionary benefits. For more information on employment information of public officials, see **section 17(2)(e)** above.

*Educational history* refers to any information regarding an individual's schooling and formal training, including names of schools, colleges or universities attended, courses taken, and results achieved.



The presumption of unreasonable invasion of privacy does not apply to certain information about enrolment in a school or program or the receipt of honours or awards. For more information about disclosure not contrary to the public interest, see **section 17(2)(j)** above.

**Personal information collected on a tax return or gathered for the purpose of collecting a tax**

**Section 17(4)(e)** This provision applies to personal information in a form used to calculate or report tax to be paid.

*Gathered for the purpose of collecting a tax* means collected by authorities for the purpose of collecting due or overdue municipal, education, federal, or provincial taxes.

**Bank account and credit card information**

**Section 17(4)(e.1)** This provision expressly refers to an individual's bank account and credit card information. Other information about an individual's financial history, such as assets, liabilities and credit history, falls within the definition of personal information and is also subject to the unreasonable invasion of privacy test. **Section 17(4)(e.1)** is intended to address concerns about the handling of electronic credit transactions and the possible misuse of credit card numbers.

In *IPC Orders F2008-014* and *F2008-015*, the Commissioner found that **section 17(4)(e.1)** applied to credit card statements that related to the third party's use of a government-issued credit card for personal use. Disclosure of some of the information was desirable for subjecting the activities of the Government of Alberta to public scrutiny. This weighed in favour of disclosing the third party's name, the dates of the transactions, and the amount of each purchase. Public scrutiny did not require disclosure of the vendors' names and locations and other transaction identifiers.

**Personal recommendations or evaluations, character references or personnel evaluations**

**Section 17(4)(f)** Personal recommendations and evaluations, as well as character references, are regularly collected by public bodies to assess an individual's employment potential. A formal process of conducting the assessment or evaluation is implied. However, recommendations and character references are also required in situations that do not involve employment. For example, references are generally required by landlords; character references are generally required before placing an individual in a position of trust.

Personnel evaluations arise most often in the employment context and include job performance appraisals and absenteeism reports.

In order for **section 17(4)(f)** to apply, the recommendations, evaluations or references must be about an identifiable individual and must be provided by someone other than that individual.

The following criteria are relevant in determining whether personal information constitutes either "personal evaluations" or "personnel evaluations".

- Was an assessment made either according to measurable standards or based upon professional judgment? (Professional judgment would be based on knowledge, training and experience.)



- Was the particular evaluation done by a person who had authority to do that evaluation?

(IPC Orders 97-002, F2008-014 and F2008-015)

In IPC Order F2002-010 **section 17(4)(f)** was found to apply to third party information that was included in a complaint about a teacher's supervision of a special-needs student at a school.

In IPC Order F2007-015, a salary increment was determined to be an evaluation because the increment was based on an assessment of the employee's performance.

***Name of individual with other personal information or that would reveal other personal information***

**Section 17(4)(g)** The disclosure of a third party's name is presumed to be an unreasonable invasion of that party's personal privacy when the name appears with other personal information about the third party (**section 17(4)(g)(i)**). In some cases, the disclosure of the name itself would reveal other personal information about the third party (**section 17(4)(g)(ii)**), such as his or her ethnic origin.

**Section 17(4)(g)** requires the record to contain a third party's name. The Commissioner has found that initials are not a name (IPC Order 99-010).

In IPC Order F2003-018, the Commissioner determined that disclosure of the names of a third party service provider's employees in a cover letter attached to a report was presumed to be an unreasonable invasion of the employees' privacy. The Commissioner found that the names either appeared with other personal information or would reveal personal information about the employees.

In IPC Order F2004-026, the Commissioner stated that **section 17(4)(g)(i)** did not apply to information that recorded the execution of an employee's work duties when that information was not evaluative or of a human resources nature, or did not otherwise have a personal dimension to it. In such circumstances, the information is not personal information. The Commissioner also stated that the names of employees were personal information, but the fact that the employees were acting in their representative capacities was a relevant circumstance that weighed in favour of disclosure.

The disclosure of the signature of a third party acting in his or representative or official capacity (e.g. a Commissioner of Oaths) is not an unreasonable invasion of the third party's personal privacy (see IPC Orders F2000-005, F2005-016 and F2007-025).

***Racial or ethnic origin or religious or political beliefs or associations***

**Section 17(4)(h)** Disclosure of an individual's racial or ethnic origin or religious or political beliefs or associations is presumed to be an unreasonable invasion of the third party's personal privacy.

*Racial origin* means information identifying common descent that connects a group of persons (e.g. Mongolian race or Caucasian descent).

*Ethnic origin* is similar to racial origin in that it identifies a common descent that connects a group of persons but extends to other common attributes such as language, culture or country of origin.

*Religious or political beliefs or associations* refers to an individual's opinions about religion or a political party, an individual's membership or participation in a church, a religious organization or political party or an individual's association or relationship with a church, a religious organization (including native spirituality), or a political party.

### **Circumstances relevant to the determination of unreasonable invasion of privacy**

**Section 17(5)** of the Act provides that, in determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy under **section 17(1)** or **(4)**, a public body must consider all the relevant circumstances, including the following.

- Is the disclosure desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny?
- Is the disclosure likely to promote public health and safety or the protection of the environment?
- Is the personal information relevant to a fair determination of the applicant's rights?
- Will the disclosure assist in researching or validating the claims, disputes or grievances of aboriginal people?
- Will the third party be exposed unfairly to financial or other harm?
- Was the personal information supplied in confidence?
- Is the personal information likely to be inaccurate or unreliable?
- Could the disclosure unfairly damage the reputation of any person referred to in the record requested by the applicant?
- Was the personal information originally provided by the applicant?

This list is not exhaustive. In applying **section 17(5)**, a public body is required to consider not only the factors listed in the provision but all the relevant circumstances. It must consider the sensitivity of the personal information in the context in which it was collected or compiled and the circumstances governing its continued protection or disclosure.

There is a growing body of Commissioner's Orders identifying relevant circumstances that are not specifically listed in the Act. These include:

- the fact that personal information is available to the public (e.g. *IPC Orders 98-001* and *F2004-015*);
- the fact that the names, titles or signatures of individuals were provided by them in their formal representative or professional capacity (e.g. *IPC Orders 2001-013*, *F2000-005* and *F2005-016*)

- the fact that the records contain only business contact information that is publicly available (*IPC F2004-026*);
- that disclosure of the information would promote the objective of providing Albertans with an open, transparent and accountable government (*IPC Order 2000-026*);
- the fact that the personal information concerned a lawsuit involving an elected official whose legal fees had been paid from public funds (*Adjudication Order No. 4*);
- the fact that a regulation of Alberta authorizes the disclosure (*IPC Order F2008-012*);
- the fact that the third party refused to consent to the disclosure of his or her personal information (e.g. *IPC Orders 97-011* and *F2008-010*); and
- the fact that the third parties are public officials (*IPC Order F2007-007*).

An applicant's prior knowledge of a third party's personal information in requested records is generally *not* a relevant circumstance (e.g. *IPC Order 96-008*).

***Circumstances weighing in favour of disclosure***

**Section 17(5)(a) *Public scrutiny.*** In some cases, the desirability of public scrutiny of the internal workings of a public body will prevail over the protection of personal privacy (see *IPC Order 97-002*). Public scrutiny is not necessarily limited to instances where wrongdoing is alleged or where it is alleged that the public body's normal practices and procedures are not being followed. It may be appropriate to disclose some personal information in order to demonstrate that the law is being properly enforced or that public policy is being carried out.

Public scrutiny of government or public body activities under **section 17(5)(a)** requires some public component, such as public accountability, public interest and public fairness (*University of Alberta v. Pylypiuk*, (2002), A.J. No. 445 (Alta. Q.B.)).

Disclosure of certain information is essential to public accountability, for example, the terms under which a police commission hires and expends public funds for a chief of police (*IPC Order F2005-016*) and the terms under which senior officials are hired by public bodies, particularly where the official is appointed to represent the province or is the chief of staff (*IPC Orders F2006-007* and *F2006-008*).

**Section 17(5)(b) *Public health, safety and protection of the environment.*** These public interests weigh in favour of disclosure for the purpose of assuring protection of the general public interest.

*Public health* refers to the wellbeing of the public at large.

The test is whether the level of physical, mental or emotional health of all or a significant part of the public would be maintained or improved by the disclosure of particular personal information.

*Public safety* refers to the safety or well-being of all or a significant part of the public.

The test is whether disclosure of personal information would reduce the community's exposure to a particular risk or danger.

*Protection of the environment* refers to guarding or defending all components of the earth – including air, land, and water; all layers of the atmosphere; all organic and inorganic matter and the interacting natural systems that include components of these things – from degradation through illegal or improper use.

**Section 17(5)(b)** is only one relevant circumstance that a public body needs to consider when determining whether disclosure of personal information is an unreasonable invasion of a third party's privacy. This circumstance alone should not be used to justify the disclosure of personal information that would clearly fall within **section 17(2)(b)**. Under that provision, if there are compelling circumstances affecting anyone's health or safety, disclosure of personal information is not an unreasonable invasion of privacy, provided notice of the disclosure is given to the third party.

The disclosure by a municipality of names and addresses of residents to a drilling company that is preparing a disaster plan as part of its requirements for an application before the Energy Resources Conservation Board would not be an unreasonable invasion of personal privacy under **sections 17(2)(c)** and **17(5)(b)**. However, the residents would have to receive written notice of the disclosure.

**Section 17(5)(c) Determination of an applicant's rights.** There may be occasions where the applicant requires access to personal information about someone else in order to assist in determining his or her own rights. Motives for requesting information are not normally relevant to the processing of a request. However, if it appears that the personal information is being requested in order to assist in determining the applicant's rights, it will be necessary for the applicant to confirm that this is the case. The interests of the applicant and the privacy interests of the third party will then have to be weighed to decide whether disclosure of personal information is essential to a fair determination of the applicant's rights.

Disclosure under this provision requires that the information be relevant to a *fair determination of the applicant's rights*. The Information and Privacy Commissioner set out the criteria for this determination in *IPC Order 99-028*. The criteria are

- the right in question must be a legal right drawn from the concepts of common law or statute;
- the right must be related to an existing or contemplated proceeding;
- the personal information being sought must have some bearing on the determination of the right in question; and
- the personal information must be required to prepare for the proceeding or to ensure an impartial hearing.

*Applicant's rights* refers to any claim, entitlement, privilege or immunity of the applicant who is requesting someone else's information. For example, disclosure of third party personal information may be necessary so that an individual can initiate legal proceedings to prove his or her inheritance rights.

*Fair* refers to administrative fairness, which is comprised of the right to know the case to be met and the right to make representations (*IPC Order F2008-012*).

An applicant's desire to pursue civil action met the requirements of the test in *IPC Order 99-028*. In a subsequent Order, however, the Commissioner gave little weight to this factor because all relevant information, other than the third party's identity, had already been disclosed to the applicant (*IPC Order F2002-010*).

**Section 17(5)(c)** will not apply where the applicant is claiming a moral right to the information, rather than a legal right under statute or common law (*IPC Order F2005-001*).

If an applicant has agreed to waive future claims on a matter, the applicant has no rights to be determined and cannot rely on this provision to pursue the matter (see *IPC Order 98-008*).

**Section 17(5)(d) *Research on or validation of the claims, disputes or grievances of aboriginal people.*** There may be a need to disclose personal information about individuals in order to research the background and expedite the settlement of wider rights for aboriginal people.

*Validating* means confirming a legally sufficient conclusion or one that has merit, based on the facts presented.

The phrase *claims, disputes and grievances* is interpreted broadly to include controversies, debates and differences of opinion regarding a range of issues, and is not restricted to differences over land claims or treaty or membership status.

*Aboriginal people* means people whose racial origins are indigenous to Canada and includes Indian, Métis and Inuit people.

***Circumstances weighing against disclosure***

**Section 17(5)(e) *Exposure to financial or other harm.*** There may be circumstances where disclosure of personal information may mean that the individual involved will be exposed unfairly to monetary loss or injury of a similar nature. The exposure would *not* be unfair, for example, where a third party writes a letter to a public body and would only be unfairly exposed to financial harm if his or her allegations were unsubstantiated (see *IPC Order 2000-026*).

Threat of a civil suit by the applicant against the third party weighed heavily against disclosure in *IPC Order F2002-010*. Disruption of family relationships or damage to the reputation of deceased individuals may also constitute harm (see *IPC Order 98-007*).

In *IPC Order F2004-016*, it was determined that harm could result from disclosure of the names of third parties who commented on the applicant's personal behaviour and work performance. Evidence indicated that the applicant would likely use the information to contact the third parties to discuss his termination of employment.

**Section 17(5)(f) *Personal information supplied in confidence.*** There are circumstances where personal information is supplied in a setting of trust and in the confidence that it will not be disclosed. Sometimes this understanding is more implicit than explicit and, in



such circumstances, the public body should attempt to protect the personal privacy of the third party. (For a detailed analysis of the meaning of “supplied in confidence”, see the discussion of **section 16(1)(b)** of the Act in this chapter.)

Some factors to consider when determining whether or not personal information was supplied in confidence are

- the existence of a statement or agreement of confidentiality, or lacking this, evidence of an understanding of confidentiality;
- the understanding of a third party as set out in his or her representations as a result of third party notice;
- past practices in the public body, particularly with regard to keeping similar personal information confidential;
- the type of personal information, especially its sensitivity and whether it is normally kept confidential by the third party; and
- the conditions under which the information was supplied by the third party, voluntarily or through informal request by the public body or under compulsion of law or regulation, and the expectations created by the collection process.

The burden of determining whether or not information was supplied in confidence lies with the public body.



Public bodies should ask their clients and organizations with which they are dealing to mark as confidential any records or parts of records containing personal information which are being supplied in confidence.

However, it is not sufficient for a public body to simply accept the stamp or assertion of a third party for confidentiality. There must be evidence to support the assertion and to prove that the personal information has been treated consistently in a confidential manner.

In *IPC Order 2000-029*, the Commissioner found that a policy assuring confidentiality does not allow a public body to withhold a third party’s personal information even if the third party supplied his or her personal information on the basis of that policy (e.g. references supplied by a third party for the purpose of admission to graduate school). The same is true of a contract.

In *IPC Order F2007-008*, the author of an e-mail intended for his identity to become public and therefore had no expectation of confidentiality. In *IPC Order F2008-012*, a physician sent an e-mail to the chief of staff of a hospital about the applicant. The physician had no reasonable expectation of confidentiality with respect to the e-mail because the e-mail could be disclosed to the applicant under the medical staff bylaws.

In *IPC Orders F2006-007* and *F2006-008*, the fact that a Treasury Board Directive required the disclosure of the salaries and benefits of senior officials meant that the third parties did not have a reasonable expectation that their salaries would be kept confidential.

There is a reasonable expectation of privacy with respect to a home address that has been provided to a public body within the context of an employment relationship (*IPC Order F2008-010*).

- Section 17(5)(g) *Inaccurate or unreliable personal information.*** A public body may have inaccurate personal information in its custody or under its control for a variety of reasons. The personal information may have been incorrectly recorded at the time of collection or compilation or it may have become inaccurate with the passage of time or as a result of a change in circumstances.

For these or other reasons, the public body may be unsure of the reliability of personal information. Such personal information should be disposed of under approved records disposition processes. Otherwise, no personal information should be disclosed from such records unless the individual concerned has consented and verified that the information is correct.

- Section 17(5)(h) *Unfair damage to reputation.*** If disclosure of personal information will unfairly damage the reputation of an individual, it should not be disclosed (see *IPC Order 97-002*).

*Unfairly* means without justification, legitimacy or equity.

*Damage the reputation* of a person means to harm, injure or adversely affect what is said or believed about the individual's character. An example of information which, if disclosed, would unfairly damage a person's reputation would be allegations of sexual harassment against an individual before an internal investigation is concluded.

This factor would weigh against the disclosure of personal information of employees in a situation where they had not been found to have acted improperly and could not defend themselves publicly (see *IPC Order 2001-001*).

The disclosure of unsubstantiated allegations may unfairly damage an individual's reputation (*IPC Order 97-002*). The damage may be less when the allegations are proven to be unsubstantiated following a formal inquiry than when the allegations have not been formally addressed (*IPC Order F2008-009*).

In *IPC Order F2006-030*, the Commissioner stated that the possibility that the disclosure of information could give rise to unfounded allegations of impropriety was not sufficient for **section 17(5)(h)** to apply.

***Other circumstances to consider***

- Section 17(5)(i) *Personal information originally provided by the applicant.*** The applicant may have provided information about an individual because the individual was in the applicant's care or custody at the time.

In most cases, **section 17(5)(i)** weighs in favour of disclosure of personal information. An example would be personal information provided to a public body by an applicant who had guardianship or trusteeship of an individual and the information was provided as a part of that responsibility (see *IPC Order 98-004*).

However, in some cases, **section 17(5)(i)** does not weigh in favour of disclosure. In *IPC Order 2000-019*, although the applicant provided the personal information of a

third party to the public body, there was a change of circumstances between the applicant and the third party. This resulted in adverse interests between the parties that led the Information and Privacy Commissioner to conclude that this factor weighed against disclosure of the personal information to the applicant.

### Existence of record

**Section 12(2)(b)** In some instances, disclosure of the mere fact that a public body maintains a record on a third party may be an unreasonable invasion of a third party's privacy.

**Section 12(2)(b)** of the Act provides that a public body may, in response to an applicant, refuse to confirm or deny the existence of a record containing personal information about a third party, if disclosing the existence of the information would be an unreasonable invasion of the third party's personal privacy.

An example would be when an applicant requests information about whether a specific individual has had a complaint lodged against him or her under a certain bylaw. If the public body locates such records and withholds them under **section 17**, informing the applicant that the records are being withheld would, by itself, tell the applicant that a complaint has been lodged against the individual.

Most public bodies will use this provision in rare instances. However, public bodies that hold sensitive personal information, such as medical or financial information, may routinely refuse to confirm or deny the existence of records containing personal information about a third party.



**When the existence of a record is neither confirmed nor denied, the response to the applicant required under section 12(1) must incorporate a statement regarding the applicant's right of review, as provided for in Model Letter J in Appendix 3.**

A refusal to confirm or deny the existence of a record is a significant limit to the right of access. If an applicant asks the Information and Privacy Commissioner to review a refusal to confirm or deny the existence of a record, the public body will be required to provide detailed and convincing reasons as to why **section 12(2)** was applied.

Before refusing to confirm or deny the existence of a record, a public body is expected to determine whether or not any record exists in order to properly fulfil its duty to assist the applicant (see *IPC Order 98-009*). A public body may not be required to conduct a search where if a responsive record was found it would necessarily contain information that would be an unreasonable invasion of personal privacy to disclose (*IPC Order F2009-002*).

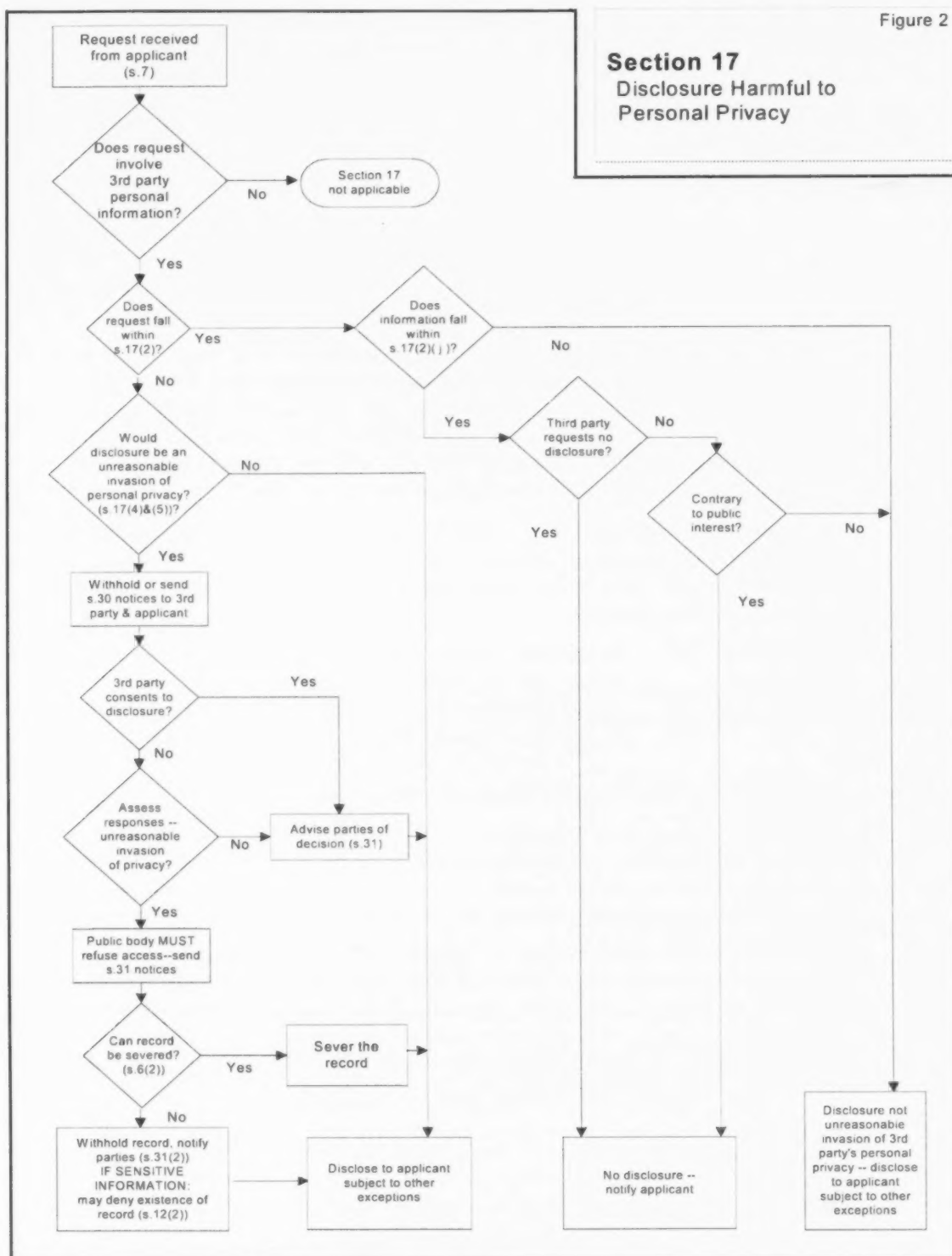
Each case must involve the exercise of discretion, not the application of a blanket policy by the public body.

### Application of exception

The application of **section 17** is set out in Figure 2. A detailed explanation of the procedures relating to third party notice that apply to this exception is provided in Chapter 5.

Figure 2

**Section 17**  
Disclosure Harmful to  
Personal Privacy



## 4.4

Disclosure  
Harmful to  
Individual or  
Public Safety**Harm to another's health or safety or interference with public safety**

**Section 18(1)** allows the head of a public body to exercise discretion to refuse to disclose information to an applicant if that disclosure could reasonably be expected to

- threaten anyone else's safety or physical or mental health (**section 18(1)(a)**); or
- interfere with public safety (**section 18(1)(b)**).

The exception may extend to an applicant's own personal information as well as to information about third parties.

In order to determine whether a threat to the safety, mental or physical health of any person exists, a public body must apply the harms test set out in *IPC Order 96-003* (see *IPC Order F2003-010*). There must be evidence of a reasonable expectation of probable harm; the harm must constitute damage or detriment; and there must be a causal connection between disclosure and the anticipated harm.

*Threaten* means to expose to risk or harm, and *safety* implies relative freedom from danger or risks.

*Mental health* refers to the functioning of a person's mind in a normal state.

*Physical health* refers to the well-being of an individual's physical body.

*Interference with public safety* would occur where the disclosure of information could reasonably be expected to hamper or block the functioning of organizations and structures that ensure the safety and well-being of the public at large.

The mental or physical health of a person would be threatened if information were disclosed to an applicant that would cause severe stress.

Individual safety could be threatened if information were released that allowed someone who had threatened to kill or injure the individual to locate him or her. Examples of individuals whose safety might be threatened would include an individual fleeing from a violent spouse, a victim of harassment or a witness to harassment, an employee who has been threatened during a work dispute or harassment case, and an individual in a witness protection program.

Mental or physical health might be threatened if information were disclosed to the applicant that could cause an individual to become suicidal or that could result in verbal or physical harassment or stalking.

In *IPC Order F2004-029*, the Adjudicator found that disclosure would result in a reasonable expectation of harm to the safety of others if investigation files relating to the applicant's complaints against police officers were disclosed. There was considerable evidence of the applicant's violent tendencies, severe mental illness and apparent lack of treatment, breach of previous court orders preventing contact with others, and frequent threats towards employees in the criminal justice system. The Adjudicator noted, however, that being difficult, challenging, troublesome, persistent, having intense feelings about injustice or, to some extent, using offensive language does not necessarily bring **section 18** into play.

Only in very rare cases will **section 18** apply to an entire record (*IPC Order F2004-029*).



### **Harm to the applicant's health or safety**

**Section 18(2)** specifically allows discretion to refuse to disclose to an applicant his or her own personal information if the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's health or safety. The decision must be supported by the opinion of a physician, a regulated member of the College of Alberta Psychologists, a psychiatrist or any other appropriate expert, depending on the circumstances of the case.

*Immediate and grave harm to an applicant's health or safety* means serious physical injury or mental trauma or danger to the applicant that could reasonably be expected to ensue directly from disclosure of the personal information.

The exception in **section 18(2)** is rarely used. Application of the exception must be based on a reasonable expectation that immediate and substantial harm would result from the disclosure of information to the individual.

An example where this exception may be relevant is where an individual with a long and difficult history of mental instability might suffer grave mental or physical trauma if certain diagnoses were made available to him or her without the benefit of medical or mental health intervention.

Under **section 6** of the FOIP Regulation, the head of a public body may disclose information relating to the mental or physical health of an individual to a medical or other expert for an opinion on whether disclosure of this information could reasonably be expected to result in grave and immediate harm to the individual's safety or mental or physical health.

When using this section, the public body must have an agreement in place to ensure that the expert maintains the confidentiality of the information. If a copy of any record is provided to the expert, it must be returned to the public body or disposed of in accordance with the agreement.

If a public body intends to disclose personal information relating to an individual's mental or physical health to a person who is a custodian under the *Health Information Act* (HIA), the public body should include a clause in the agreement stating that the information disclosed under the agreement is personal information subject to the *FOIP Act* (not HIA).

Though the intent of **section 18(2)** is to ensure that the applicant does not receive personal information that might cause immediate and grave trauma, efforts should be made to provide to the applicant as much of his or her own personal information as possible.

After obtaining the expert opinion, the public body may require the applicant to examine the requested record in person, and in the presence of someone who can clarify the information and assist the applicant in understanding it. That person may be a medical or other expert, a member of the applicant's family, or some other person approved by the public body (**section 6(5)** of the FOIP Regulation).

### **Information about individual health or safety supplied in confidence**

**Section 18(3)** allows a public body to refuse to disclose information that reveals the identity of an individual who has provided confidential information about a threat to someone's safety or mental or physical health.

This discretionary exception allows a public body to protect the identity of experts and of informants who provide such information. Examples of individuals whose identity might have to be protected include a person reporting abuse under the *Protection for Persons in Care Act*, or a person reporting suicidal tendencies of a student.

### **Existence of record**

In some instances, disclosure of the mere fact that a public body maintains a record may reasonably be expected to threaten someone else's safety, interfere with public safety, or even cause harm to the applicant.

**Section 12(2)(a)** of the Act provides that a public body can refuse to confirm or deny the existence of a record containing information described in **section 18**.



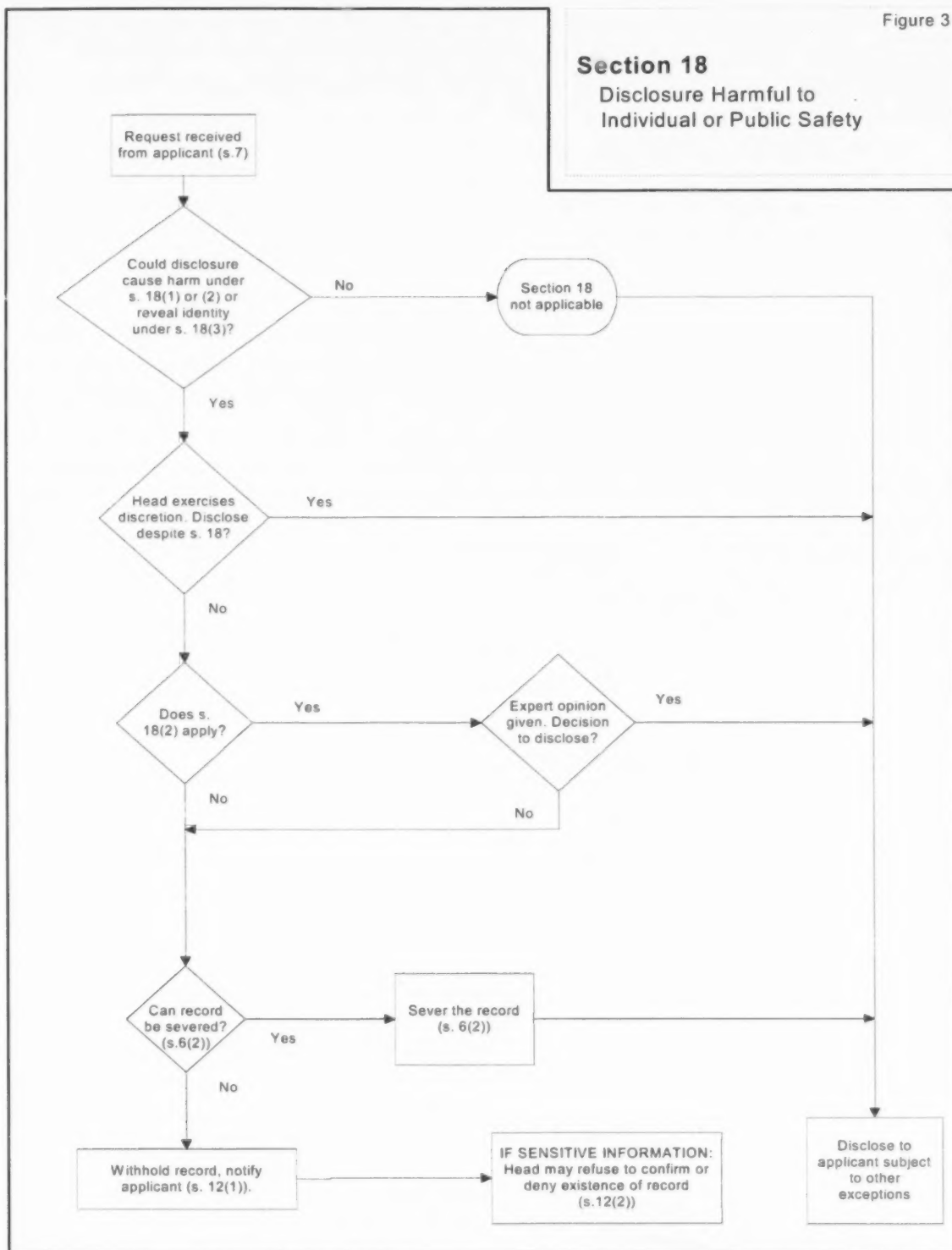
**When the existence of a record is neither confirmed nor denied, the response to the applicant, as required under section 12(1), must incorporate a statement regarding the applicant's right of review as provided for in Model Letter J in Appendix 3.**

For more information on neither confirming nor denying the existence of a record, see section 4.3 of this chapter.

### **Application of exception**

Figure 3 contains a flowchart setting out the application of **section 18**.

Figure 3



## 4.5

Confidential  
Evaluations

**Section 19** of the Act provides that a public body may refuse to disclose to an applicant confidential evaluative information or opinions, such as an opinion in an employment reference, in certain circumstances.

**Section 19** is a discretionary exception and applies only when an individual is requesting his or her own personal information. The exception applies to both the applicant's own personal information and the personal information of the individual supplying the evaluation or opinion. The exception is intended to preserve the candour of the evaluative information or opinions.

### Confidential evaluations for employment, contracts or other benefits

*Section 19(1)* The application of **section 19(1)** is subject to a three-part test:

- information must be evaluative or opinion material;
- information must be compiled for the purpose of determining the applicant's suitability, eligibility or qualifications for employment, or for the awarding of contracts or other benefits by a public body; and
- information must be provided, explicitly or implicitly, in confidence.

(See *IPC Orders 98-021* and *2000-029*.)

This provision protects the process where information is compiled about an individual in order to assess his or her suitability for either employment or the awarding of contracts or other benefits. This may involve information on his or her personal strengths or weaknesses, or eligibility (fitness or entitlement), or qualifications (attainments and accomplishments). The exception applies only to the selection process and not to evaluative processes relating to other aspects of employment or the awarding of contracts or benefits.

*Employment* refers to selection for a position as an employee of a public body, as defined in the Act (**section 1(e)**).

*Contracts* refer to agreements relating to both personal services and the supply of goods and services.

*Other benefits* refer to benefits conferred by a public body through an evaluative process. The term includes research grants, scholarships and prizes. It also includes appointments required for employment in a particular job or profession such as a bailiff or special constable (see *IPC Order 98-021*).

The term is not intended to refer to admission to programs of study, student or low-income housing, or benefits based solely on objective criteria.

For example, a post-secondary educational institution cannot withhold access to an applicant's reference letter regarding admission to a graduate program (see *IPC Order 2000-029*). However, the same institution could withhold a reference letter provided in confidence for the purpose of a competition for a post-doctoral position, which is a paid research position, not an educational program (*IPC Order F2002-027*).

For this exception to apply, the personal information must be contained in a confidential evaluation or opinion provided to the public body. If the public body has compiled a summary of confidential evaluations or references, the summary would also qualify for this exception (see *IPC Order 98-021*).

Examples of confidential evaluations to which **section 19(1)** may apply include:

- a verbatim transcription of a reference check of an employment candidate;
- a summary of a mix of telephone and written reference checks compiled by a public body employee;
- recorded comments from a third party who is not a referee for a candidate but makes the comments in the same employment context in which a reference letter would be provided (*IPC Order F2003-007*); and
- handwritten notes taken by an interviewer during the recruitment process (*IPC Order F2004-022*).

An analysis of an interview with a prospective candidate or of all reference checks prepared by the public body would not qualify for this exception. Factual information such as statistics on absenteeism would also not be withheld under this exception.

#### **Confidential information for employee evaluation**

*Section 19(2) and (3)* **Section 19(2)** provides an exception to disclosure for personal information of participants in a formal employee evaluation process concerning the applicant.

The application of **section 19(2)** is subject to a three-part test:

- the information must be provided by a participant in a formal employee evaluation process concerning the applicant;
- the information must be provided, explicitly or implicitly, in confidence; and
- the information must be personal information that identifies or could reasonably identify the participant (*IPC Order F2006-025*).

*Participant* is defined in **section 19(3)** as including a peer, subordinate or client of the applicant. It does not include the applicant's supervisor or superior. **Section 19(3)** may apply to an external assessor in an academic promotion process (*IPC Order F2006-025*).

Public bodies that incorporate "360 degree" evaluations into performance appraisals may withhold the names and positions of subordinates or colleagues, or the identity of students or clients of the applicant.

**Section 19(2)** is distinct from **section 19(1)**. **Section 19(2)** is not intended to allow the withholding of the evaluative or appraisal information itself. However, in certain situations, such as those involving a very small review group, some or all of the evaluative comments may reasonably be expected to reveal the identity of the reviewer and may be withheld under **section 19(2)**. (See *IPC Order F2006-025*.)

Reference checks relating to a current employee who is a candidate in an employment competition are not considered to be made for the purpose of a performance review



but rather to determine the individual's suitability, eligibility or qualifications for employment in another position. Information provided by the employee's current supervisor would not be considered information for a formal evaluation process as contemplated under **section 19(2)**. This information should be considered under **section 19(1)** (*IPC Order F2002-008*).

#### **Information provided in confidence**

For either **section 19(1)** or **section 19(2)** to apply, the information must be provided with either an explicit or implicit understanding that it will be held in confidence. This intention that confidentiality will be maintained may be explicitly stated in the record itself or in an agreement governing the process, or implied by the circumstances under which the information has been collected.

Where confidentiality is implied, there must be objective grounds to support the assumption of confidentiality. It is not sufficient for the submitting party simply to stamp documents "Confidential." Public bodies are encouraged to have written policies regarding whether certain processes are considered to be confidential, and procedures in place to protect the anonymity of individuals involved in such processes.

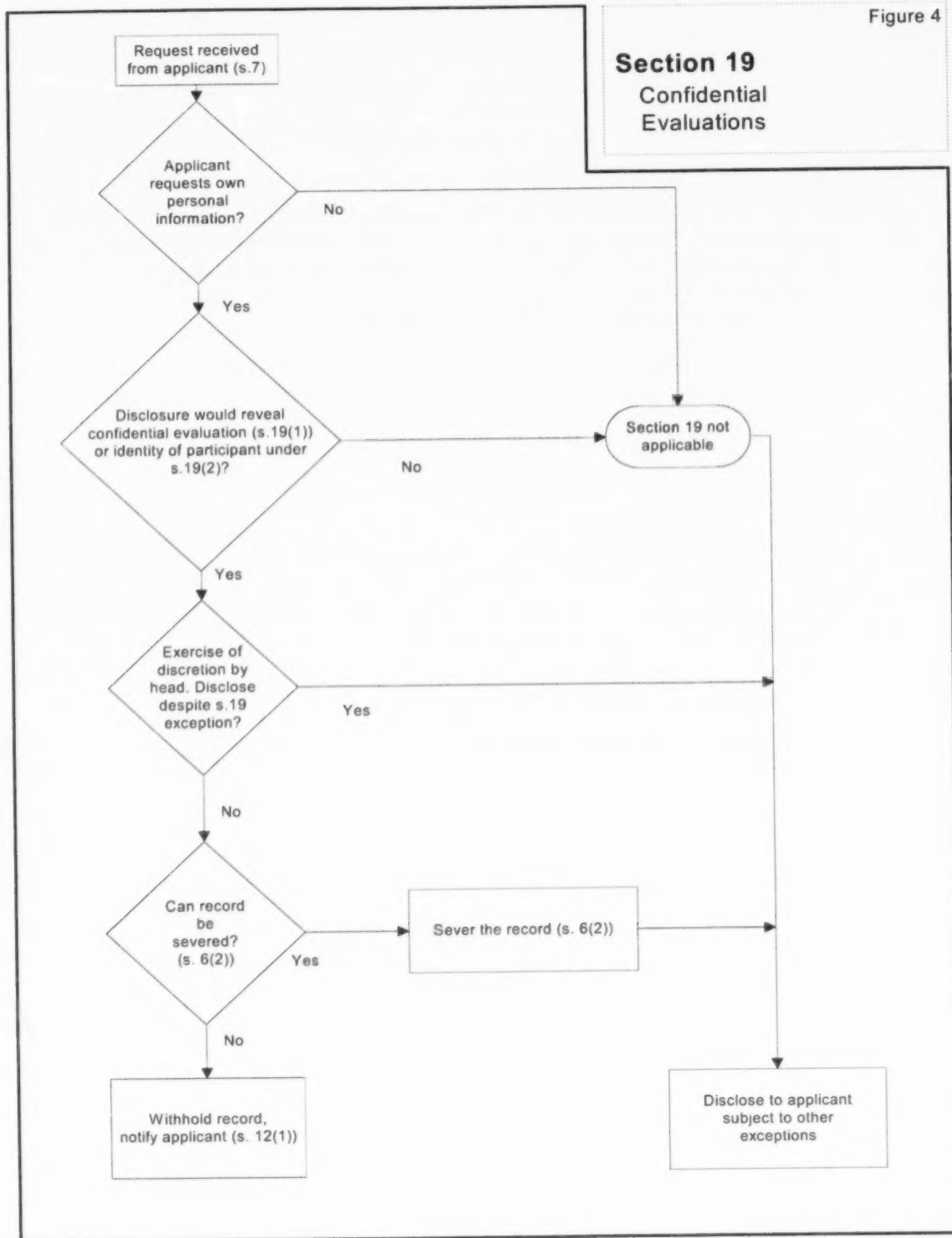
Although an evaluation may have been provided in confidence, a public body may still exercise its discretion to disclose the evaluation if no other exception applies.

Some factors that may be considered when determining whether information was supplied in confidence are set out in section 4.2 of this chapter.

#### **Application of exception**

Figure 4 contains a flowchart setting out the application of **section 19**.

Figure 4



#### 4.6 Disclosure Harmful to Law Enforcement

**Section 20** of the Act deals with the application of exceptions to protect both law enforcement activities and information in certain law enforcement records. It contains a number of discretionary exceptions, and a mandatory exception requiring public bodies to refuse to disclose information if this would be an offence under an Act of Canada. For a more detailed discussion of this exception, see FOIP Bulletin No. 7: *Law Enforcement*, published by Access Privacy, Service Alberta.

#### Definition of law enforcement

*Law enforcement* is defined in **section 1(h)** of the Act as

- policing, including criminal intelligence operations;
- a police, security or administrative investigation, including the complaint that gives rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred; or
- proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred.

*Policing* refers to the activities of police services. This means activities carried out under the authority of a statute regarding the maintenance of public order, detection and prevention of crime or the enforcement of law (see *IPC Order 2000-027*).

*Criminal intelligence* is information relating to a person or group of persons. It is compiled by police services to anticipate, prevent or monitor possible criminal activity. Intelligence-gathering is sometimes a separate activity from the conduct of investigations. Intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, or to ensure the security of individuals or organizations.

*Investigation* has been defined, in general, as a systematic process of examination, inquiry and observation (*IPC Orders 96-019 and F2002-024*).

A *law enforcement investigation* is an investigation that leads or could lead to a penalty or sanction. The phrase *lead or could lead* in this definition allows for investigations to be considered law enforcement even if they do not ultimately result in proceedings before a court or tribunal.

The Information and Privacy Commissioner has ruled that, for the purposes of the *FOIP Act*, the investigation must be one that can result in a penalty or sanction imposed under a statute or regulation (*IPC Order 2000-023*, affirming *IPC Order 96-006*). The Office of the Commissioner has interpreted this restriction to include penalties or sanctions imposed under a bylaw enacted under a statute (*IPC Investigation Report F2002-IR-009*).

The *penalty or sanction* may include a fine, imprisonment, revocation of a licence, an order to cease an activity, or expulsion from an educational institution.

An investigation relating to a breach of contract or a contravention of a policy by an employee will not normally constitute a law enforcement activity, since these actions would not result in a penalty or sanction under a statute or regulation.

For example, in *IPC Order 2000-019*, the Commissioner said that although an investigation of a breach of employment duties was an administrative investigation carried out under section 25 of the *Public Service Act*, the disciplinary action that could result would not be law enforcement because the duties were not set out in an enactment that provides for penalties or sanctions in the event of a breach.

Under **section 1(h)** of the Act, an investigation includes the complaint that triggers the investigation. This means that the initial complaint receives the same consideration, if protection from disclosure is required, as the rest of the investigation.

The law enforcement exception may be applied when a body other than the one carrying out the investigation has authority to impose the penalty or sanction. This includes a body such as the RCMP or another federal agency that is not a public body, as defined in the *FOIP Act*.

To apply the law enforcement exception, public bodies will need to ensure that a specific authority to investigate is in place and that the investigation can lead to a penalty or sanction being imposed. Three types of investigations are specifically included: police, security and administrative investigations.

A *police investigation* is one carried out by the police, or other persons who carry out a policing function that involves investigations. For example, a police investigation may include an investigation by a special constable appointed under the *Police Act*, or by a person responsible for investigating possible regulatory offences under a federal or provincial enactment such as the *Criminal Code* (Canada) or the *Traffic Safety Act*.

A *security investigation* includes an activity carried out by, for, or concerning a public body and relates to the security of the organization and its clients, staff, resources, or the public. Security includes the work that is done to secure, ensure safety or protect from danger, theft or damage. A security investigation will fall within the scope of the law enforcement exception only if it is conducted under the authority of a statute, regulation, bylaw or other legislative instrument which includes a penalty or sanction for the offence investigated.

An *administrative investigation* is a formal investigation carried out to enforce compliance or to remedy non-compliance with standards, duties and responsibilities. These standards, duties and responsibilities must be defined under an Act, regulation, bylaw or other legislative instrument, which must also include a penalty or sanction for the non-compliance under investigation.

The regular day-to-day review and monitoring of employee performance, including employee grievances, would generally not be considered an administrative investigation for the purposes of the Act's definition of law enforcement. A civil action for monetary damages or recovery of a debt, or an internal employment-related investigation does not fall within this section.

Investigations performed under the authority of a federal or provincial Act or regulation that can result in a prosecution would generally be considered to be part of law enforcement. The specific facts of the matter would determine whether it was a police, security or administrative investigation.

Examples of administrative investigations include

- an inspection under the *Water Act* (IPC Order F2002-024)
- an investigation by Environment Canada into the discharge from a landfill site owned by a municipality (IPC Order F2005-013)
- an investigation under the *Traffic Safety Act* and the Operator Licensing and Vehicle Control Regulation to determine whether an individual could safely operate a motor vehicle (IPC Investigation Report F2007-IR-004)
- a complaint made and an investigation conducted under the *Protection of Persons in Care Act* (IPC Order F2005-009)

A public body need not carry out the investigation for that investigation to meet the definition. The investigation might be carried out by a police service on behalf of the public body. If the requested records are not within the custody or control of the public body to which the request is made, that public body is not required to search for responsive records in the custody or under the control of another public body (see IPC Order 2001-013).

*Proceedings* include an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions concerning a person's rights. This includes administrative proceedings before agencies, boards and tribunals.

### **Exception for law enforcement information**

**Section 20(1)** is a discretionary exception. It provides that a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

- harm a law enforcement matter;
- prejudice the defence of Canada or of any foreign state allied to or associated with Canada;
- disclose activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act* (Canada);
- harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement;
- reveal the identity of a confidential source of law enforcement information;
- reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities;
- interfere with or harm an ongoing or unsolved law enforcement investigation, including a police investigation;
- reveal any information relating to prosecutorial discretion;



- deprive a person of the right to a fair trial or impartial adjudication;
- reveal a record that has been confiscated from a person by a peace officer in accordance with a law;
- facilitate the escape from custody of an individual who is being lawfully detained;
- facilitate the commission of an unlawful act or hamper the control of crime;
- reveal technical information relating to weapons or potential weapons;
- harm the security of any property or system, including a building, a vehicle, a computer system or a communications system; or
- reveal information in a correctional record supplied, explicitly or implicitly, in confidence.

The application of the exception under several of the provisions of **section 20(1)** is subject to a test for harm. See section 4.1 of this chapter for a discussion of the harms test and IPC FOIP Practice Note 1: *Applying "Harms" Test*.

***Harm a law enforcement matter***

**Section 20(1)(a)** This provision permits a public body to refuse disclosure of information that may result in harm to law enforcement activities.

*Harm* implies damage or detriment (see *IPC Order 2001-010* for a discussion of the meaning of harm generally). The harm threshold is designed to protect law enforcement while preserving the public's right of access to some types of law enforcement information.

A public body contemplating a decision to withhold information needs to be able to demonstrate that there is a reasonable likelihood of harm if the specific information is disclosed. The likelihood of harm will depend, in part, on the sensitivity of the law enforcement information.

To invoke this exception, a public body must establish a direct link between the disclosure of specific law enforcement information and the harm that is expected to result from the disclosure. It cannot simply claim harm to law enforcement in general (see *IPC Order 96-003*).

A public body does not need to demonstrate that actual harm will result or that actual harm resulted from similar disclosures in the past. However, past experience is a valuable indicator of the expected harm.

Generally, this provision is used to protect law enforcement investigations that are active. It may also be used to protect the confidentiality of the process through which complaints are received.

***Prejudice the defence of Canada or of any foreign state allied to or associated with Canada***

**Section 20(1)(b)** This provision allows a public body to refuse disclosure of information that could reasonably be expected to be detrimental to national defence or to Canada's international relations with respect to defence matters.

*Prejudice* in this context refers to detriment to national defence. The test for prejudice is not as demanding as the test for harm.

*Defence of Canada* means any activity or plan relating to the defence of Canada, including improvements in the nation's ability to resist attack.

An *allied state* is one with which Canada has concluded formal alliances or treaties.

An *associated state* is one with which Canada may be linked for trade or other purposes outside the scope of a formal alliance.

Public bodies in Alberta hold only limited information related to national defence. However, the presence of military installations within the province and cooperation between the federal and provincial governments for emergency planning are matters that could fall within the scope of this exception.

***Disclose activities suspected of constituting threats to the security of Canada***

**Section 20(1)(b.1)** This provision allows a public body to withhold information that could disclose activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act* (Canada). Threats to the security of Canada include

- espionage or sabotage, or supporting activities, against Canada or detrimental to the interests of Canada;
- foreign-influenced activities detrimental to the interests of Canada that are clandestine or deceptive or involve a threat to any person;
- activities within or relating to Canada that threaten or use acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective; and
- activities directed toward undermining the constitutionally established system of government in Canada by covert unlawful acts or violence.

These activities do not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the listed activities.

*Espionage* is any activity carried out by spies or related to spying.

*Sabotage* is malicious or wanton destruction, usually, but not always, directed against property. Property may include computers, computer programs and data.

**Section 20(1)(b.1)** permits a public body to refuse to disclose information that could reasonably be expected to disclose activities that are *suspected* of constituting threats to the security of Canada. The public body is not required to meet the harms test to apply this exception.

Examples of information to which this exception may apply include information relating to suspected activities intended to cause serious damage to critical infrastructure in the public or private sector, such as bombings of oil field installations, and information concerning local security planning for a meeting of heads of state or an international sporting event.

A public body wishing to rely on this exception to disclosure should consult with other government departments or agencies that specifically deal with threats of this nature.

***Harm the effectiveness of investigative techniques and procedures***

**Section 20(1)(c)** This provision permits a public body to refuse disclosure of information that could harm the effectiveness of investigative techniques used, or likely to be used, in law enforcement.

**Section 20(1)(c)** recognizes that unrestricted access to law enforcement techniques could reduce their usefulness, effectiveness and success.

*Investigative techniques and procedures* means techniques and procedures used to conduct an investigation or inquiry for the purpose of law enforcement (*IPC Order F2007-005*)

Since this exception is subject to the harms test, a public body cannot rely on **section 20(1)(c)** to refuse to disclose basic information about well-known investigative techniques, such as wire-tapping, fingerprinting and standard sources of information about individuals' addresses, personal liabilities, real property, etc. (*IPC Orders 99-010 and F2003-005*).

If a technique or procedure is generally known to the public, disclosure would not normally compromise its effectiveness (*IPC Order 2000-027*).

The exception is more likely to apply to new technologies in electronic monitoring or surveillance equipment used for a law enforcement purpose. The exception extends to techniques and procedures that are *likely to be used*, in order to protect techniques and technology under development and new equipment or procedures that have not yet been used.

***Reveal the identity of a confidential source***

**Section 20(1)(d)** This provision enables a public body to refuse to disclose information that reveals the identity of a confidential source of law enforcement information. The fact that the information, if disclosed, could reveal the identity of a confidential source is sufficient to apply this exception. The information need not be law enforcement information. There is no need to demonstrate that harm could come to the source.

*Identity* includes the name and any identifying characteristics, symbols and numbers relating to the source.

A *confidential source* is someone who supplies law enforcement information, as defined in the Act, to a public body with the reasonable expectation that his or her identity will remain secret. Employees, whether directly employed or under contract, cannot be *sources* because they are a part of a public body and are supplying information as part of their jobs (see *IPC Order 99-010*).

Where a public body can demonstrate that there is a confidential source of information and that the information supplied by the source is law enforcement information, the public body must then determine whether the particular information requested could permit the applicant or anyone else to identify the source. Since it is

often difficult to determine whether information can be linked to establish identification, caution should be exercised in releasing any information connected to a confidential source.

If the identity of a confidential source of law enforcement information appeared in a law enforcement record, disclosure of the individual's identity would be a presumed unreasonable invasion of personal privacy under **section 17(4)(b)**. A public body would have to determine whether the factors in **section 17(5)**, as well as any other relevant circumstances, weigh in favour of disclosing the identity. The presumption of unreasonable invasion would not arise when the disclosure of the identity of the confidential source of law enforcement information is necessary to dispose of the law enforcement matter or to continue an investigation.

The public body could apply the discretionary exception under **section 20(1)(d)** as an additional exception. It is a good practice to apply all applicable discretionary exceptions initially so that the public body is not prohibited from doing so later in a review process.

If police informer privilege applies, the identity of the informant is considered to be privileged information and must not be disclosed since it is subject to **section 27(2)**, a mandatory exception to disclosure. For further information on police informer privilege, see section 4.13 of this chapter.

#### ***Reveal criminal intelligence relating to organized criminal activities***

**Section 20(1)(e)** This provision allows a public body to refuse disclosure of information that could reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of

- organized criminal activities; or
- serious and repetitive criminal activities.

*Criminal intelligence* is information relating to a person or group of persons compiled by law enforcement agencies to anticipate, prevent or monitor possible criminal activities.

Intelligence-gathering is often unrelated to the investigation of a specific offence. For example, intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, and for ensuring the security of individuals or organizations. Intelligence may be drawn from investigations of previous incidents that may or may not have resulted in the trial and conviction of the person under surveillance.

*Organized criminal activities* occur when a group of individuals come together with the intent of committing crimes or when they conspire together to commit crimes. There is a degree of organization or deliberate planning involved, which is not the case with random criminal acts. Examples may include the activities of gangs and automobile theft rings, smuggling narcotics, and transporting illegal immigrants.

*Serious and repetitive criminal activities* occur when the same person, or group of persons, commit serious crimes repeatedly. The criminal activity has to be one that carries a heavy penalty or has a major impact on society or individuals. Examples

include serial bank robberies, dealings in illegal drugs and ongoing industrial sabotage.

This exception does not require an expectation of harm. A public body wishing to rely on this exception would have to be able to demonstrate a rational relationship between the information collected and the operations for which that information may be used.

***Interfere with or harm an ongoing or unsolved investigation***

**Section 20(1)(f)** This provision allows a public body to refuse to disclose information that could either interfere with or harm an ongoing or unsolved investigation.

*Interfere with* is a less stringent test than the harms test under **section 20(1)(a)**. It includes hindering or hampering an ongoing investigation and anything that would detract from an investigator's ability to pursue the investigation.

The exception applies to ongoing or active investigations and those where investigative activity has ceased but the crime remains unsolved. This includes investigations where a prosecution has not resulted, but does not include those where charges were dropped. An example would be an unsolved murder or a fraud investigation. An investigation has been found to be ongoing where the public body had not yet decided whether to seek a prosecution (*IPC Order F2005-026*) and where the Crown Prosecutor has the files and is considering whether to proceed with charges (*IPC Order F2004-023*).

The public body must demonstrate the harm that would result from disclosure (see the discussion of **section 20(1)(a)** above), or the way in which disclosure would interfere with or hinder the investigation.

***Reveal information relating to the exercise of prosecutorial discretion***

**Section 20(1)(g)** This provision allows a public body to refuse to disclose information related to the exercise of discretion by Crown Counsel or a special prosecutor with regard to prosecuting an offence.

*Prosecutorial discretion* means the exercise of a prosecutor's discretion related to his or her power to prosecute, negotiate a plea, withdraw charges, enter a stay of proceedings, and appeal a decision or verdict (see *IPC Orders 2001-011, 2001-030 and 2001-031*). Prosecutorial discretion involves the ultimate decision as to whether a prosecution should be brought, continued or ceased, and what the prosecution ought to be for, that is, the nature and extent of the prosecution and the Attorney General's participation in it (*IPC Order F2006-005*, citing the Supreme Court of Canada in *Krieger v. Law Society of Alberta* [2002] 3 S.C.R. 372]).

The exercise of prosecutorial discretion may be with respect to offences under the *Criminal Code* (Canada) and any other enactment of Canada for which the Minister of Justice and Attorney General for Alberta may initiate and conduct a prosecution. Prosecutorial discretion may also be exercised with respect to offences under an enactment of Alberta, including prosecution of provincial regulatory offences.



Most records relating to this exception will be in the custody or under the control of Alberta Justice. Copies of records or notes reflecting the discretion exercised may be in the files of other public bodies, especially police services.

The fact that information is in a Crown Prosecutor's files does not necessarily mean that the information relates to the exercise of prosecutorial discretion. The substance, not location, of the information is determinative (*IPC Order F2007-021*).

**Section 20(2)** states that this exception does not apply to information that has been in existence for 10 years or more. For a discussion on the application of time limitations to exceptions, see section 4.1 of this chapter. Information that would qualify for exception under **section 20(1)(g)** but which is 10 or more years old must be disclosed unless another exception applies to it.

***Deprive of the right to a fair trial or impartial adjudication***

**Section 20(1)(h)** This provision enables a public body to refuse to disclose information that could reasonably be expected to deprive a person of the right to a fair trial or impartial adjudication. The exception applies to a person.

*Person* includes an individual, a corporation, a partnership and the legal representatives of a person.

*Fair trial* refers to a hearing by an impartial and disinterested tribunal that renders judgment only after consideration of the evidence, the facts, the applicable law and arguments from the parties.

*Impartial adjudication* means a proceeding in which the parties' legal rights are safeguarded and respected.

This exception applies not only to civil and criminal court actions but also to proceedings before tribunals established to adjudicate individual and collective rights. Examples of proceedings before tribunals include hearings before the Labour Relations Board, and hearings of human rights panels.

In applying the exception, the public body must present specific arguments about how and why disclosure of the information in question could deprive a person of the right to a fair trial or hearing. Commencement of a legal action is not by itself enough to support the application of this exception.

***Reveal a record confiscated by a peace officer***

**Section 20(1)(i)** This provision permits a public body to refuse disclosure that would reveal a record that has been seized from a person by a peace officer in accordance with the law.

**Section 20(1)(i)** applies to records confiscated from individuals, corporations and partnerships, and their representatives.

A *peace officer* is defined in section 1(j) of the *Police Act* to mean a person employed for the purposes of preserving and maintaining the public peace. Other laws set out what the term *peace officer* means in relation to those laws (e.g. *Peace Officer Act*). A peace officer could include a mayor, sheriff or sheriff's officer, warden, correctional officer, and any other officer or employee of a penitentiary, prison or

correctional centre. It also includes a police officer, police constable and a special constable.

The record must have been confiscated under the authority of a law. An example would be business records of a company seized by a peace officer investigating suspected tax fraud.

***Facilitate escape from custody***

**Section 20(1)(j)** This provision allows a public body to refuse disclosure of information if the disclosure could reasonably be expected to facilitate the escape from custody of a person who is lawfully detained.

*Lawfully detained* means being held in custody pursuant to a valid warrant or other authorized order. Persons lawfully detained would include:

- persons in custody under federal or provincial statute;
- young persons in open or secure custody or pre-trial detention under the *Alberta Youth Justice Act*;
- persons involuntarily committed to psychiatric institutions; and
- parole violators held under a warrant.

The exception also extends to individuals remanded in custody (i.e. charged but not yet tried or convicted). It does not apply to individuals released under bail supervision.

An example of information protected by this exception is the building plans for a correctional facility.

In order to apply this exception, the public body must establish a reasonable expectation that disclosure of the information could facilitate an escape from custody. In *IPC Order F2007-005*, there was no evidence that disclosure of a training video relating to a police canine unit could facilitate an escape.

***Facilitate the commission of an unlawful act***

**Section 20(1)(k)** This provision permits a public body to refuse to disclose information that would be of use in committing a crime or that could hamper the control of crime. Examples include information about techniques, tools and instruments used for criminal acts, names of individuals with permits for guns, the location of police officers, and the location of valuable assets belonging to a public body.

A public body must be prepared to demonstrate how or why disclosing the information in question could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime. Also, the Commissioner may examine whether, on the face of the records, there is a reasonable possibility that disclosure of the information would result in the alleged consequence (*IPC Order F2004-032*).

***Reveal technical information relating to weapons***

**Section 20(1)(l)** This provision enables a public body to refuse to disclose information that could reasonably be expected to make the applicant or others aware of technical

information relating to weapons or to materials that have the potential to become weapons. For example, this exception would cover information on how to make a bomb.

***Harm the security of property and systems***

**Section 20(1)(m)** This provision permits a public body to refuse to disclose information that could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system, and a communications system. This exception is subject to the harms test (see the discussion of the harms test in section 4.1 of this chapter).

*Security* generally means a state of safety or physical integrity. The security of a building includes the safety of its inhabitants or occupants when they are present in it. Examples of information relating to security include methods of transporting or collecting cash in a transit system, plans for security systems in a building, patrol timetables or patterns for security personnel, and the access control mechanisms and configuration of a computer system.

**Section 20(1)(m)** has been applied where disclosure of information could be expected to harm the security of communication systems and codes used by the Calgary Police Service in relation to its law enforcement records (*IPC Order F2005-001*). The exception did not apply to a chapter of a police procedural manual where the information relating to the execution of search warrants was common knowledge (*IPC Order F2004-032*).

***Reveal information in a confidential correctional record***

**Section 20(1)(n)** This provision enables a public body to refuse to disclose all or part of a record that could reasonably be expected to reveal information in a correctional record supplied explicitly or implicitly in confidence.

A *correctional record* refers to information collected or compiled while an individual, either an adult or young person, is in the custody or under the supervision of correctional authorities or their agents as a result of legally imposed restrictions. It includes records relating to

- imprisonment;
- parole;
- probation;
- community service orders;
- bail supervision; and
- temporary absence permits.

The correctional record itself need not be in the custody or control of the public body. The exception may apply if the information would reveal information that is in the correctional record. The information may be an extract from the record or a summary of the record. To qualify for the exception, the information must have been supplied in confidence. This means that there is an agreement or understanding between the parties or some longstanding practice governing how the information will be treated.

This may be explicit, in that it has been agreed to in writing, or implicit, in that both parties assume the confidentiality.

It is not sufficient to simply mark the information as being received in confidence. There must be evidence that a condition of confidentiality is a normal part of the process of supplying the information. For more information on confidentiality, see section 4.3 of this chapter.

**Exposure to civil liability or harm to the proper custody or supervision of an individual**

*Section 20(3)* **Section 20(3)** is also a discretionary exception. It allows non-disclosure of information that could expose an individual to civil liability or could harm the proper custody or supervision of an individual under correctional supervision.

***Exposure to civil liability***

*Section 20(3)(a)* **Section 20(3)(a)** allows a public body to refuse to disclose information to an applicant if the information is in a law enforcement record and the disclosure could reasonably be expected to expose the author of the record, or an individual quoted or paraphrased in the record, to civil liability.

This exception protects law enforcement officials, and those providing information to them, from civil suit as a result of disclosure of records made in the course of carrying out law enforcement activities (see *IPC Order 2001-027*).

***Harm to the proper custody or supervision of an individual under the control of a correctional authority***

*Section 20(3)(b)* **Section 20(3)(b)** allows a public body to refuse disclosure of information about the history, supervision or release of a person who is in custody or under the supervision of a correctional authority. The exception applies only if disclosure could reasonably be expected to harm the proper custody or supervision of that person. The same harms test is required as for **section 20(1)(a)**, discussed above.

*History* means information about the person such as an employment record or medical information.

*Supervision* refers to the overseeing of a person.

The provision applies to adults and young persons still subject to control by correctional authorities or their agents as a result of legally imposed restrictions on their liberty. This includes individuals in prison, on parole, on probation, on a temporary absence permit, under bail supervision or performing community service work. The exception allows discretion to except specific information about someone in custody or under supervision.

Examples include information regarding security arrangements for the transfer of a prisoner between facilities, whether or not a prisoner is in a public hospital, and the appointment of a probation officer.



This exception cannot be used to deny access to an applicant who is no longer in custody and is seeking his or her own personal information.

### Disclosure is an offence under an Act of Canada

**Section 20(4)** **Section 20(4)** is a mandatory exception. It provides that a public body must refuse to disclose information to an applicant if the information is in a law enforcement record and the disclosure would be an offence under an Act of Canada.

*Law enforcement record* means any recorded information relating to law enforcement as defined in the Act.

A disclosure is an *offence under an Act of Canada* if a federal statute prohibits the disclosure and makes it an offence. An offence under a federal regulation or other subordinate legislation does not fall within this category.

Examples of such Acts are

- the *Youth Criminal Justice Act* (Canada), which makes it an offence to knowingly disclose certain court, police, government and other records relating to young offenders except as authorized by that Act;
- the *Security of Information Act* (Canada), which prohibits disclosure of information that could prejudice the security of the country; and
- the *Criminal Code* (Canada), which prohibits the release of wiretap transcripts.

### When the exception does not apply

**Section 20(5)** **Section 20(5)** of the Act provides that **section 20(1)** and **section 20(3)** do not apply to

- a report prepared in the course of routine inspections by an agency that is authorized to enforce compliance with an Act of Alberta (**section 20(5)(a)**); or
- a report, including statistical analysis, on the degree of success achieved in a law enforcement program, unless disclosure of the report could reasonably be expected to interfere with or harm the matters referred to in **section 20(1)** or **20(3)**.

The intent of **section 20(5)** is to encourage disclosure of reports and statistics about law enforcement programs.

*Routine inspections* involve scheduled inspections by public officials to ensure that standards or other regulatory requirements are being met. They take place without specific allegations or complaints having been made. Examples include inspections under the *Safety Codes Act*, public health inspections, fire inspections, liquor licensing inspections, and safety inspections on trucks or school buses under the *Traffic Safety Act*.

Such reports are usually factual in nature and report the conditions found by the inspector. They may include advice or other information that could be excepted under other sections of the Act.



Reports and statistics on the success of law enforcement programs should be routinely disclosed whenever possible. Only if the contents of the report could interfere with or harm any of the matters set out in the preceding sections would information be withheld. This would be done by severing the appropriate parts of the report.

Examples of statistical law enforcement reports include information on programs such as "Crimestoppers" and "Checkstop," statistics on elevator safety inspections, and reports on matters such as the success in preventing abuse of handicapped parking stalls.

### **Completed investigations**

*Section 20(6)* **Section 20(6)** of the Act provides that, after a police investigation is completed, a public body may disclose the reasons for the decision not to prosecute

- to a person who knew of and was significantly interested in the investigation, including a victim or a relative or friend of a victim (**section 20(6)(a)**); or
- to any other member of the public, if the fact of the investigation was made public (**section 20(6)(b)**).

There is no general requirement to disclose information about decisions not to prosecute unless the investigation itself was made public. To apply **section 20(6)(b)**, there would have to be evidence of this fact, such as a newspaper report about the investigation or a news release.

The provision relates only to police investigations and not to the whole field of law enforcement.

### **Existence of record**

*Section 12(2)* There are situations in which the disclosure of the mere existence of a record could result in harm to law enforcement. For example, disclosure of the existence of investigation records or criminal intelligence may indicate that enforcement activities are being undertaken and this, in itself, could harm those activities.

**Section 12(2)(a)** of the Act provides that a public body may, in response to an applicant, refuse to confirm or deny the existence of a record containing information described in **section 20**.

In order to rely on **section 12(2)(a)**, a public body must first consider what interest would be protected by withholding the record under **section 20** and then consider whether refusing to say if such information exists would promote or protect the same interest. In other words, the public body must be able to show that disclosure of whether the information exists or not would result in one of the negative consequences in **section 20** (*IPC Orders F2006-012, F2006-013 and F2006-015*).



When the existence of a record is neither confirmed nor denied, the response to the applicant, as required under section 12(1)(c) of the Act, must include a statement regarding the applicant's right of review. (See Model Letter J in Appendix 3.)

See section 4.3 of this chapter ("Existence of a record") for a discussion of **section 12(2)(b)**.

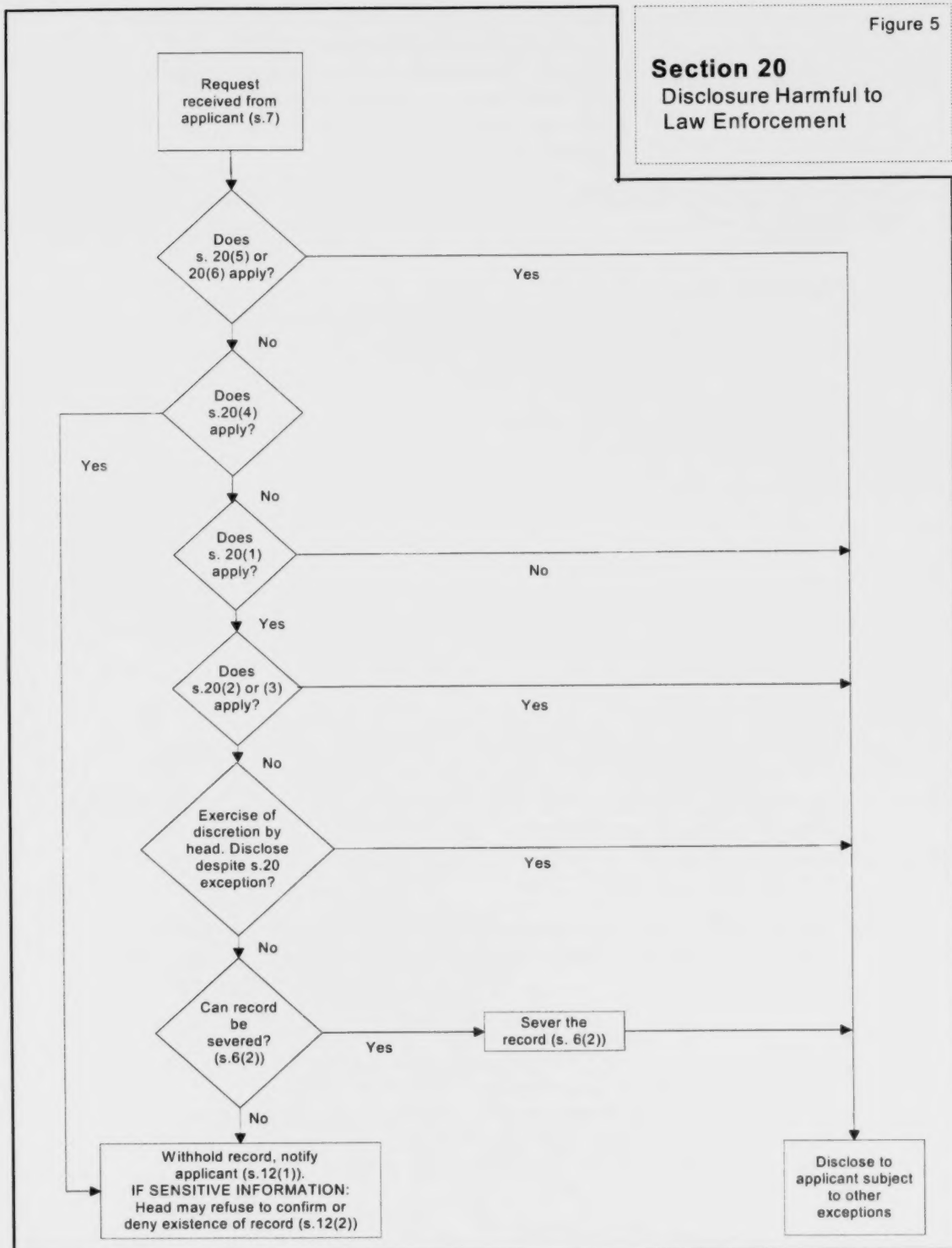
#### **Application of exception**

Figure 5 contains a flowchart setting out the application of **section 20**.

Figure 5

## Section 20

Disclosure Harmful to Law Enforcement



#### 4.7 Disclosure Harmful to Intergovernmental Relations

**Section 21** provides that a public body may refuse to disclose information that could harm intergovernmental relations or the intergovernmental supply of information. This is a discretionary exception.

This exception has two parts, one dealing with harm to relations and the other with information given in confidence.

**Section 21(1)** allows a public body to refuse access if disclosure could reasonably be expected to

- harm relations between the Government of Alberta or its agencies and any of the following or their agencies:
  - the Government of Canada or a province or territory of Canada,
  - a local government body, as defined in the *FOIP Act* (see section 1.1. of Chapter 1),
  - an aboriginal organization that exercises government functions,
  - the government of a foreign state, or
  - an international organization of states (**section 21(1)(a)**);

or

- reveal information supplied explicitly or implicitly in confidence by a government, local government body or an organization listed above or its agencies (**section 21(1)(b)**).

#### Consultation

Consultation regarding whether or not to invoke this exception should normally take place between the FOIP Coordinator of the public body and officials in comparable positions in external government bodies.



**Where the federal or foreign governments, aboriginal organizations or international organizations are involved, consultations must be conducted in cooperation with Alberta International and Intergovernmental Relations or Alberta Aboriginal Relations.**

Where local governments are involved, consultation would occur with the appropriate public body, as indicated by the nature of the records. Public bodies that will need to consult on a regular basis should establish practices and contact points to expedite the process.

#### Harm to intergovernmental relations

**Section 21(1)(a)** This provision applies to information that if disclosed could reasonably be expected to harm relations between the Government of Alberta and the listed external government entities. The exception may apply to information that relates to current or future relations.

*Relations* is intended to cover both formal negotiations and more general exchanges and associations between the Government of Alberta and other governments or their agencies.

*Harm* means damage or detriment to negotiations and general associations and exchanges. To satisfy the harms test, there must be a reasonable probability that disclosure would harm and not merely hinder, impede or minimally interfere with the conduct of intergovernmental relations or negotiations.

Although information exchanged between provincial and federal ministers may be sensitive, in order to apply **section 21(1)(a)**, a government body must be able to provide evidence or an argument that disclosure would harm relations between the Government of Alberta and the Government of Canada (see *IPC Order 2001-006*).

The term *Government of Alberta* has a broader sense here than an individual provincial government department or agency. The exception has a different and higher-level coverage, in that *government* is intended to convey the sovereign power of the state in carrying out its will and functions. Public bodies wishing to invoke **section 21(1)(a)** must demonstrate that the conduct of intergovernmental relations of the Government of Alberta, and not just those of the public body, would be harmed by the disclosure.

The exception relates to government bodies external to the Government of Alberta, to certain aboriginal organizations and to local government bodies.

The exception also covers any of their agencies (i.e. corporate bodies or persons designated by any of the listed external government organizations). For example, the Department of National Defence is an agency of the Government of Canada, UNESCO is an agency of the United Nations, and an economic development agency is an agency of a local government.

The provision covers not only *provincial governments* but also *territorial governments* (e.g. the Government of the Yukon) and their agencies.

An *aboriginal organization* refers to the council of a band as defined in the *Indian Act* (Canada) and any organization established to negotiate or implement, on behalf of aboriginal people, a treaty or land claim with the federal government. This definition in relation to treaties and land claims does not limit the subject matter of the records to which the exception may apply. The particular records need not deal with treaties or land claims. An example of other types of records may be the results of achievement tests of students in band schools.

A *foreign state* refers to the government of any foreign nation or state, including the component state governments of federated states.

An *international organization of states* refers to any organization with members representing and acting under the authority of the governments of two or more states. Examples include the United Nations and the International Monetary Fund.

An example of information that might qualify for this exception is notes of private discussions between officials of a city, its twinned counterpart in a developing



country, the province and the country concerned, where no agreement has been reached between the parties to make the discussions public.

### **Disclosure of information**

**Section 21(2)** Section 21(2) of the Act states that information referred to in **section 21(1)(a)** may be disclosed only with the consent of the Minister responsible for the *FOIP Act* (i.e. the Minister of Service Alberta) in consultation with the Executive Council.



**Where a public body wishes to disclose information that qualifies for the exception set out in section 21(1)(a), it must prepare a submission describing the information and setting out the circumstances and reasons why it wishes to disclose this information.**

The submission should be prepared in consultation with

- Alberta International and Intergovernmental Relations, where records concerning the federal government, foreign governments or international organizations are involved;
- Alberta Aboriginal Relations, where records concerning aboriginal organizations, such as First Nations, are involved; or
- Alberta Municipal Affairs or other relevant department, where local governments are involved, and

with the other government, as appropriate.

This submission must then be signed by the head of the public body and submitted to the Minister of Service Alberta for consideration. If, after discussing the matter with the public body and with other appropriate departments, the Minister of Service Alberta believes that disclosure should take place, the Minister and the head of the relevant Alberta Government department will jointly sponsor the submission to the Executive Council for consideration. After this consultation, the Minister will either consent to, or deny, the application.

### **Information supplied in confidence**

**Section 21(1)(b)** This provision provides for the non-disclosure of information that could reasonably be expected to reveal information received in confidence from one of the bodies specified in **section 21(1)(a)**. A decision that a confidence would be revealed is enough to satisfy the test here. It is not necessary that the harms test set out in **section 21(1)(a)** also be met (*IPC Order F2004-018*).

In order to be covered by **section 21(1)(b)**, the information must have been supplied in circumstances that clearly place an obligation on the public body to maintain confidentiality.

*In confidence* usually describes a situation of mutual trust in which private matters are related or reported. Criteria for determining whether information has been given, explicitly or implicitly, in confidence are provided in section 4.2 of this chapter.

The public body has the burden of proving that the information was submitted in confidence.

Examples of information that may be supplied in confidence include:

- information exchanged between the Canadian Security Intelligence Service and municipal police forces;
- correspondence about and transcripts of a confidential meeting of the western Premiers; and
- negotiating strategies relating to a federal, provincial and municipal infrastructure program.

A public body's awareness that the information may be disclosed during a future disciplinary hearing or criminal prosecution does not affect the understanding that the information was supplied to the public body in confidence (*IPC Order F2004-018*).

Where multiple governments supplied information to a database that was only accessible to authorized users (including an Alberta Government department) under the terms of an agreement that facilitates the enforcement of consumer legislation, and the agreement contained express consent and privacy provisions, the Information and Privacy Commissioner found that the information was supplied explicitly in confidence (*IPC Order 2001-037*).

#### **Disclosure of information**

**Section 21(3)** **Section 21(3)** of the Act provides that a public body may disclose information supplied in confidence only with the consent of the government (provincial, territorial or foreign), the local government body, the organization or the agency that supplied the information. If consent has not been obtained, **section 21(3)** precludes disclosure (*IPC Order 96-004*).

Consultation with the other party or parties providing the information should take place between officials who are authorized to make decisions about the disclosure. The consent of the government, local government body, organization or agency that provided the information should be in writing.

#### **Time limitation**

**Section 21(4)** This provision states that **section 21** does not apply to information that has been in existence in a record for 15 years or more. For a further discussion on the application of time limitations to exceptions, see section 4.1 of this chapter.

Information qualifying for exception under **section 21** but which is 15 or more years old must be disclosed unless another exception applies to it.

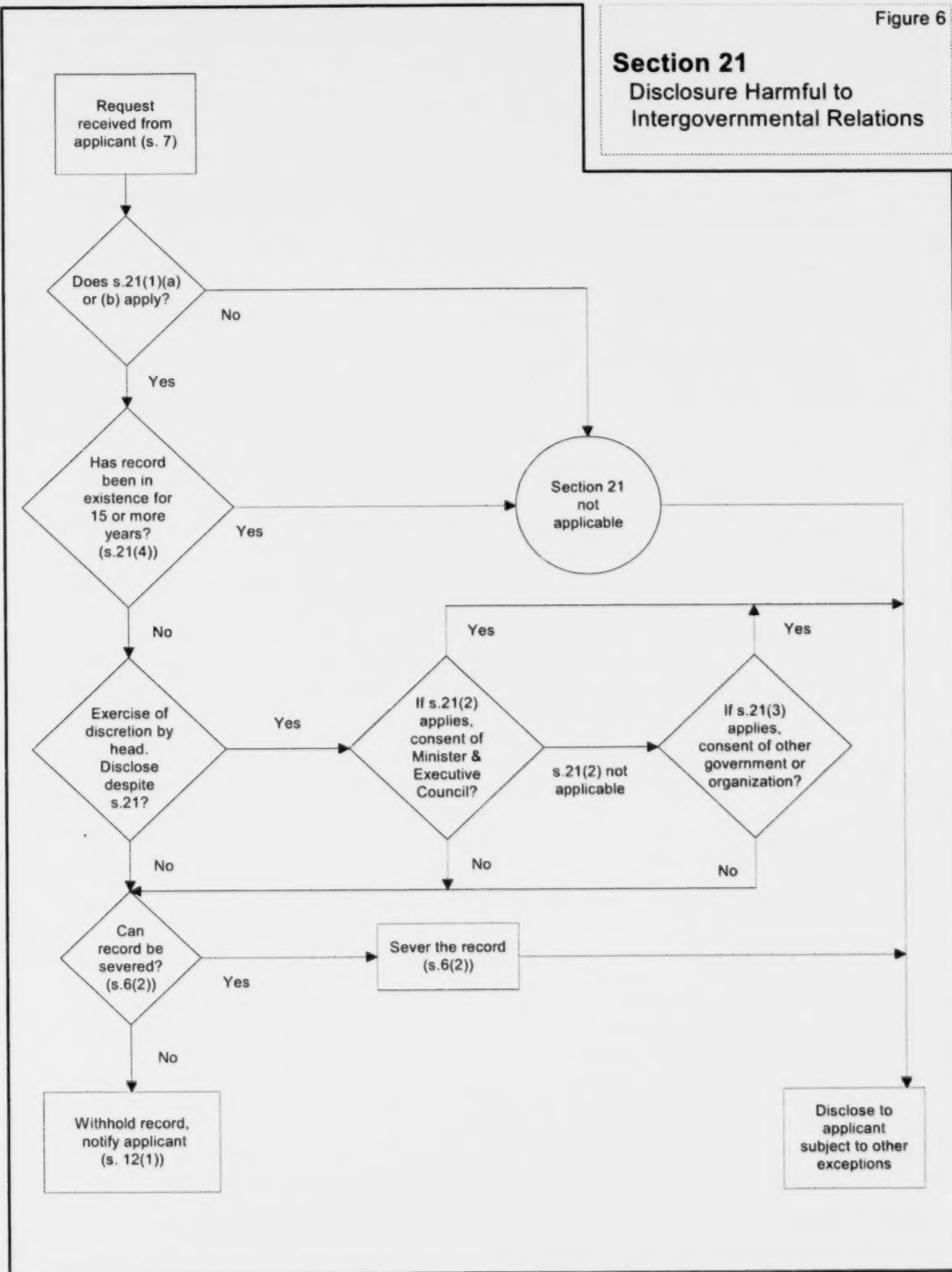
#### **Application of exception**

Figure 6 contains a flowchart setting out the application of **section 21**.

Figure 6

## Section 21

### Disclosure Harmful to Intergovernmental Relations



**4.8  
Cabinet and  
Treasury Board  
Confidences**

**Section 22(1)** sets out a mandatory exception for information that would reveal the substance of deliberations of the Executive Council or any of its committees. The exception also applies to the Treasury Board or any of its committees. A public body must refuse to disclose to an applicant any advice, recommendations, policy considerations or draft legislation or regulations submitted to or prepared for submission to these bodies.

*Executive Council* is commonly known as the provincial Cabinet and refers to the ministers and the Premier acting collectively.

**Section 22(1)** does not apply to information submitted to or prepared for submission to an individual member of the Executive Council, unless the individual minister is carrying out the direction of Cabinet or is acting as a Cabinet committee.

*Treasury Board* refers to the Treasury Board itself, not the department of the same name. The role of the Treasury Board is set out in the *Financial Administration Act*.

*Committees of the Executive Council* include the Agenda and Priorities Committee, certain standing committees, except for Cabinet Policy Committees, and ad hoc committees struck to deal with specific issues.

*Committees of the Treasury Board* refers to similar committees.

Cabinet Policy Committees (CPCs) are not considered Cabinet committees. When information flows among Cabinet, Treasury Board and CPCs, it is often difficult to distinguish the origins and purpose of particular information. In dealing with CPC records, or records created for CPCs, **sections 22, 24** (advice and recommendations) and **4(1)(q)** (which excludes some CPC information from the scope of the Act) must be applied in concert with each other.

*Advice* includes the analysis of a situation or issue that may require action and the presentation of options for future action, but not the presentation of facts.

*Recommendations* includes suggestions for a course of action as well as the rationale for a suggested course of action.

*Policy considerations* refers to matters taken into account in deciding on a course or principle of action.

*Draft legislation or regulations* refers to preliminary versions of legislative instruments, such as draft Acts, regulations to be enacted pursuant to statutory authority, and Orders to be enacted under the authority of the Lieutenant Governor in Council (O.C.s).

The listing of categories of information and records to which **section 22(1)** may apply (advice, recommendations, policy considerations, and draft legislation or regulations) is not exhaustive. These are examples of types of information that would be likely to reveal deliberations of the Executive Council, Treasury Board or their committees.

The purpose of the exception for Cabinet and Treasury Board confidences is to preserve the unique role of Cabinet institutions and conventions within the framework of parliamentary government in Alberta. This role is based on the

principle of collective ministerial responsibility to the Legislature and the people of the province for the actions of the government.

To facilitate this collective decision-making, Cabinet deliberations have traditionally been kept confidential. This permits full and frank discussions around the Cabinet table. The confidentiality of the decision-making process also allows for the appropriate timing of announcements of decisions.

Because **section 22** deals with the Cabinet process, the Office of the Executive Council makes all decisions as to whether information meets the criteria for applying the exception with respect to the Executive Council or its committees. The Department of Treasury Board makes all decisions as to whether information meets the criteria for applying the exception with respect to the Treasury Board or its committees. The requirement to consult with the Department of Treasury Board applies only to information that would reveal the substance of deliberations of the Treasury Board or its committees, not to information that the Treasury Board requires departments to prepare, such as business plans.



**Consultation on confidences of the Executive Council must be conducted through the office of the FOIP Coordinator, Office of the Executive Council. Consultation on confidences of the Treasury Board must be conducted through the FOIP Coordinator, Department of Treasury Board.**

### **Reveal the substance of deliberations**

**Section 22(1)** The exception to disclosure for Cabinet and Treasury Board confidences applies to information “that would reveal the substance of deliberations.”

*Substance* means the essence, the material or essential part of a deliberation (see *IPC Orders 97-010 and 99-002*).

*Deliberation* means the act of weighing and examining the reasons for and against a contemplated action or course of conduct or a choice of acts or means (see *IPC Orders 97-010 and 99-002*).

Information would *explicitly* reveal the substance of deliberations if the information itself contained the essence or material part of the deliberations, for example, a transcript, a report, or a summary.

Information would *implicitly* reveal the substance of deliberations if the information could reasonably be combined with other information to reveal the essence or material part of the deliberations.

To qualify for this exception, the record or information must deal with issues that will be or have been discussed by the Executive Council, the Treasury Board or one of the committees of either body. In addition, the public body must demonstrate that the records would reveal the substance of the deliberations. It is not sufficient for the public body to merely speculate that the records would *likely* reveal the substance of the Cabinet’s discussions (*IPC Order F2004-026 and F2007-013*).



**Section 22(1)** does not apply to records that make reference to past and future Cabinet meetings but which do not reveal the substance of Cabinet deliberations at those meetings (see *IPC Order 99-040*).

Where a public body has not provided a record for the purpose of submission to Cabinet, the public body cannot rely on this exception, because disclosure of the records would not reveal the substance of Cabinet deliberations (see *IPC Order 2001-008*). **Section 22(1)** would not apply to the names of persons who prepared the material for Cabinet or the dates or topics of the deliberations unless that information would, in itself, reveal the substance of the deliberations (*IPC Orders F2004-026*).

Examples of records that would reveal the substance of deliberations of the Executive Council, Treasury Board or one of their committees are

- agendas, minutes and related documents of Executive Council meetings;
- letters and memoranda referring to deliberations upon or decisions taken by ministers but not made public (although these may have been sent to ministerial colleagues or senior public servants);
- briefing material, exclusive of background facts, placed before the Executive Council, the Treasury Board or one of their committees;
- a draft or final submission to the Executive Council or the Treasury Board, excluding background facts (see *IPC Order 2000-013*);
- a memorandum (including e-mail) from the Secretary to Cabinet ministers discussing Cabinet decisions;
- a memorandum (including e-mail) from a deputy minister to an assistant deputy minister or chief executive officer or other senior officer dealing with issues that will be or have been deliberated upon by the Executive Council, the Treasury Board or one of their committees;
- a record of discussions between senior officials about issues that will be or have been deliberated upon by the Executive Council, the Treasury Board or one of their committees; and
- a briefing note from a deputy minister or chief executive officer to a minister concerning what will be, or has been, discussed in Executive Council, the Treasury Board or one of their committees.

**When the exception does not apply**

**Section 22(2)** sets out various circumstances where **section 22(1)** does not apply.

**Information in a record in existence for 15 years or more**

**Section 22(2)(a)** The exception in **section 22(1)** applies only to records or portions of records that have been in existence less than 15 years. Other exceptions may apply to particular information in these records.

*15 years* means the period from a particular month and day to a corresponding month and day 15 years later.

**Information in a record of a decision made by Executive Council or any of its committees on an appeal**

- Section 22(2)(b)** Where the Executive Council or one of its committees functions as an appeal body under an Act and makes a decision, the decision and any recorded reasons for the decision are available to the public. Other portions of the record, such as the advice and recommendations supporting the deliberative process leading to a decision, remain subject to **section 22(1)**.

**Background facts**

- Section 22(2)(c)** The exception for Cabinet and Treasury Board confidences does not apply to information in a record if the purpose of the information is to present background facts to the Executive Council, Treasury Board, or any of their committees, for consideration in making a decision and if

- the decision has been made public;
- the decision has been implemented; or
- five years or more have passed since the decision was made or considered.

This provision permits the disclosure of information prepared specifically with the intent of presenting factual information (i.e. explanations of situations, as opposed to advice, recommendations, or policy considerations or analysis) to the Executive Council, the Treasury Board or any of their committees.

*Background facts* means facts that provide explanatory or contextual information. Background facts are usually found in attachments to submission documents and are intended to assist Cabinet in its deliberations. For example, if a record was not prepared to present recommendations or proposals to Cabinet but rather for a use unrelated to the Cabinet deliberative process (such as newspaper clippings, tables of statistics or reports prepared for use within a department), and provided to Cabinet for information only, it could not be excepted under **section 22(1)** simply because it was attached to a memorandum distributed to Cabinet (*IPC Order 97-010*). Information that would reveal the substance of deliberations of the Executive Council, the Treasury Board, or any of their committees, such as summaries of background materials that highlight issues and key implications for deliberations, would not constitute background facts for the purposes of this provision. The background facts remain subject to **section 22(1)** (see *IPC Order 2000-013*).

**Section 22(2)(c)** does not allow public bodies to except background facts from disclosure if one of three criteria apply.

First, the exception for Cabinet and Treasury Board confidences does not apply to background facts if the decision has been made public.

A decision *has been made public* if it has been communicated to the public in an authorized way. Communication to the public in an authorized way would include communication in a statement by a minister, a statement or release by a communications officer, a statement in Question Period, a presentation in the Legislative Assembly, or a letter or statement to the media. A "leak" of information is not considered an authorized disclosure of information.

Second, the exception for Cabinet and Treasury Board confidences does not apply to information providing background facts if the decision has been implemented.

A decision *has been implemented* if the decision has been put into effect (see, for example, *IPC Order 99-040*). A decision is not considered to have been implemented if the decision remains subject to approval or is not final. A decision has been implemented if it has been acted upon, even if action with respect to the subject of the decision is not complete.

For example, if the Treasury Board decided to go forward with a government-wide spending cut, implementation would commence when a plan of action was communicated to departments. At that time, the background facts would cease to be protected by **section 22(1)**.

In cases where decisions are reconsidered, clarified, amended, reversed or delayed, the exception does not apply to background facts if the decision that has subsequently been reconsidered has either been made public or implemented. However, other provisions of the Act may prevent disclosure.

The Commissioner has noted that, in applying **section 22(2)(c)**, it is necessary to examine the context in which a record containing background facts was presented to Cabinet. The fact that a decision on a particular subject has been made public does not mean that background facts respecting a related decision can be disclosed. One must consider precisely what decision was being deliberated when the background facts were submitted to Cabinet (see *IPC Order 97-010*).

Third, the exception for Cabinet and Treasury Board confidences does not apply to background facts if 5 or more years have passed since the decision was made or considered.

*5 years* refers to a time period from a particular month and day to a corresponding month and day 5 years later.

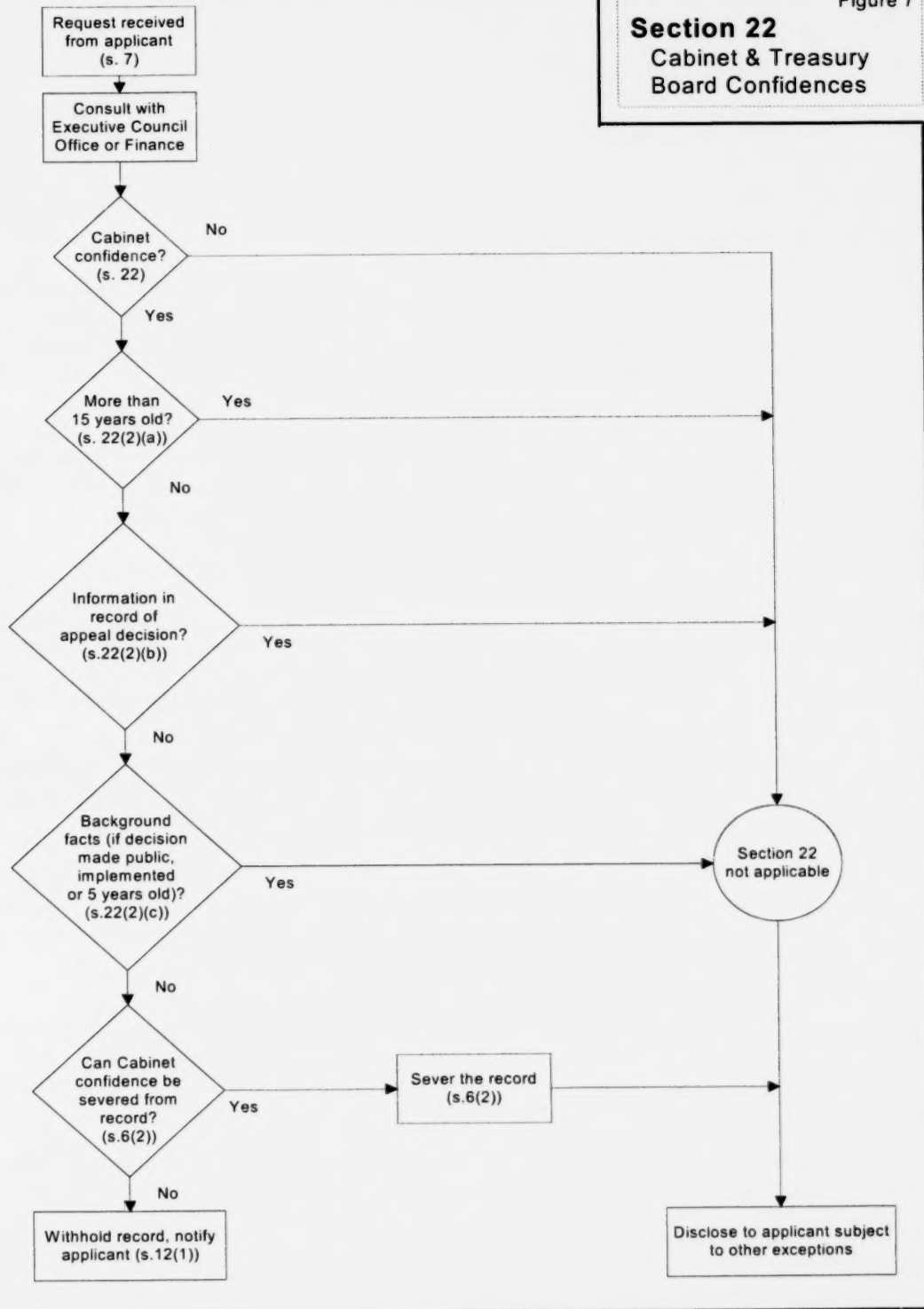
This exception to the general rule of confidentiality for Cabinet and Treasury Board deliberations applies regardless of whether or not a decision has been made public or has been implemented. If the background facts were presented to the Executive Council, the Treasury Board or any of their committees for consideration in making a decision, and 5 years have elapsed, the exception to disclosure for the background information under **section 22(1)** does not apply. However, as noted above with respect to the meaning of "background facts," it is necessary to consider whether factual information falls within the meaning of background facts or whether the factual information would reveal the substance of deliberations.

### **Application of exception**

Figure 7 contains a flowchart setting out the application of **section 22**.

Figure 7

## Section 22 Cabinet & Treasury Board Confidences



**4.9  
Local  
Public Body  
Confidences**

**Section 23(1)** of the Act provides that a local public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to reveal

- a draft of a resolution, bylaw or other legal instrument by which the local public body acts; or
- the substance of deliberations of a meeting of its elected officials or governing body or a committee of its governing body, if an Act or a regulation under the *FOIP Act* authorizes the holding of that meeting in the absence of the public.

**Section 23** is a discretionary exception.

For example, an applicant may request a copy of a memorandum sent by the chair of a committee of a college board to committee members. The memorandum in question discusses a number of administrative matters and also discusses an issue that the committee must discuss at a forthcoming meeting that will not be open to the public. The information relating to this latter issue may be severed from the record if it would reveal the substance of deliberations of the committee on a matter specified in the FOIP Regulation or in the local public body's governing Act as one that may be considered *in camera*. The applicant would receive the remainder of the record unless other exceptions applied to it.

**Draft resolution, bylaw or other legal instrument**

**Section 23(1)(a)** This provision extends to legal instruments of a local public body the same protection extended to provincial government legislation and regulations in **section 24(1)(e)**.

*Draft* means a version of the resolution, bylaw or other legal instrument that has not been finalized for consideration in public by the local public body.

The exception may be applied to the whole draft record or to individual sections or clauses. An example would be a preliminary version of a land use bylaw drafted by a staff member for the consideration of a municipal council.

A *resolution* means a formal expression of opinion or will of an official body or public assembly, adopted by a vote of those present. The term is usually employed to denote the adoption of a motion such as an expression of opinion, a change to rules or a vote of support or censure.

For example, an official of a school district may draft a resolution setting out amended rules for the operation of individual schools. This amendment to the rules goes through several internal drafts before it is presented to the school board for discussion and consideration for approval. All versions other than the version that is submitted to the board may be withheld under this provision.

A *bylaw* means a rule adopted by a local public body with bylaw-making powers, such as a municipal council.

*Other legal instrument* by which a local public body acts is intended to cover other legal or formal written documents, other than resolutions or bylaws, that relate to the internal governance of a local public body or the regulation of the activities over which it has jurisdiction.



While drafts may be withheld under this exception, the final version of the bylaw, resolution or other legal instrument cannot.

### **Substance of deliberations of *in camera* meetings**

**Section 23(1)(b)** *Substance* means the essence or essential part of a discussion or deliberation (see *IPC Order 97-010*).

*Deliberation* means the act of weighing and examining the reasons for and against a contemplated act or course of conduct. It also includes an examination of choices of direction or means to accomplish an objective (see *IPC Order 97-010*).

*Meeting* means an assembly or gathering at which the business of the local public body is considered. It includes both the meeting in its entirety and a portion of a meeting (see **section 1(4)** of the FOIP Regulation).

*Elected officials* means those individuals publicly elected through a balloting process to conduct the business of the local public body.

*Governing body* means the assembly of persons that is responsible for the administration of the local public body.

In relation to a post-secondary educational institution, the term *governing body* is defined in **section 4(2)** of the *FOIP Act*, as meaning

- the board of governors or general faculties council of a university, as described in the *Post-secondary Learning Act*; or
- the board of governors or academic council of a public college or technical institute, as described in the *Post-secondary Learning Act*.

*Committee of its governing body* means a group of people who have been designated by the governing body of the local public body to act on its behalf and consider a particular issue or subject (e.g. a collective bargaining or negotiating committee). A committee may be composed of elected officials or appointed members of the local public body.

In order for information relating to a meeting held *in camera* to qualify for this exception,

- the disclosure of information would have to reasonably be expected to reveal the substance of deliberations of a meeting of the public body's elected officials or of the public body's governing body or a committee of its governing body; and
- the holding of the meeting in the absence of the public
  - is authorized by an Act of Alberta (not a regulation, rule or bylaw made under that Act); or
  - is in accordance with **section 18** of the FOIP Regulation.

Under **section 23(1)(b)** of the Act, if there is no specific provision relating to *in camera* meetings in the Act that establishes and governs a local public body, then information may be excepted from disclosure only if the subject matter considered in

the absence of the public concerns, and is limited to, a matter specified in **section 18** of the FOIP Regulation, namely

- security of the property of the public body;
- personal information of an individual, including an employee of the public body;
- the proposed or pending acquisition or disposition of property by or for the public body;
- labour relations or employee negotiations;
- a law enforcement matter (as defined in **section 1(h)** of the Act), litigation or potential litigation, including matters before administrative tribunals; or
- consideration of a request for access to information under the *FOIP Act* if the governing body or committee is itself designated as the head of the local public body.

**Section 18** of the FOIP Regulation applies, for example, to post-secondary educational bodies, which do not have provisions relating to *in camera* meetings in their governing legislation. It does not apply to public bodies subject to the *Municipal Government Act*, which has its own provision related to the holding of *in camera* meetings.

In *IPC Order 2001-040*, a bylaw of a police commission was found to be a regulation, not an Act that authorized the holding of a meeting of the commission in the absence of the public. However, the Acting Commissioner found that **section 18(1)** of the FOIP Regulation applied to the holding of the *in camera* meetings that were the subject of an applicant's request. The Acting Commissioner also held that the records of those meetings fell within the scope of the exception in **section 23(1)(b)**.

In *IPC Order F2004-015*, the Commissioner found that it was unclear whether a certain committee of the Board of Trustees had the authority under section 70 of the *School Act* to meet in private. The Committee could not rely on **section 18(1)** of the FOIP Regulation for authorization to meet in public because the subject matter of the meeting did not fall within one of the prescribed categories.

*In the absence of the public* means in the absence of the public at large. A meeting may still be considered to be held in the absence of the public if it is attended by a member of a local public body who is not an elected official, member of the governing body or member of a committee of the governing body.

A meeting that may be held *in camera*, but to which certain members of the public are specifically invited to discuss sensitive issues pertaining to their property or themselves or their rights, is a meeting held in the absence of the public. However, a meeting that is permitted to be held *in camera*, but to which is made open to the public, is not a meeting held in the absence of the public.

A meeting open to the public, which no members of the public happen to attend, is also not a meeting held in the absence of the public.

Common types of records relating to *in camera* meetings that may be protected are agendas, minutes, notes made by participants, and other records that document the substance of deliberations within such meetings.

Records that may be the subject of discussions, such as a report detailing an investigation into a complaint against a teacher, or a proposal from a company for tax concessions in return for a development project, could not normally be withheld under this exception. However, the substance of deliberations about such documents may be withheld. This information will usually be part of other records and will have to be severed from them.

#### **When the exception does not apply**

*Section 23(2)(a)* The exception in **section 23(1)(a)** does not apply where the draft of the resolution, bylaw or other legal instrument has been considered in a meeting open to the public. This means that, if a particular draft is discussed in a public meeting, there is no reason to deal with the information under an exception. Prior or subsequent drafts that are not considered in a public meeting can still be withheld under this exception.

*Section 23(2)(b)* The exception in **section 23(1)(b)** does not apply where the subject matter of the deliberation has been considered in a meeting open to the public. This means that, where a local public body has not explicitly excluded the public from the meeting, the exception cannot be applied.

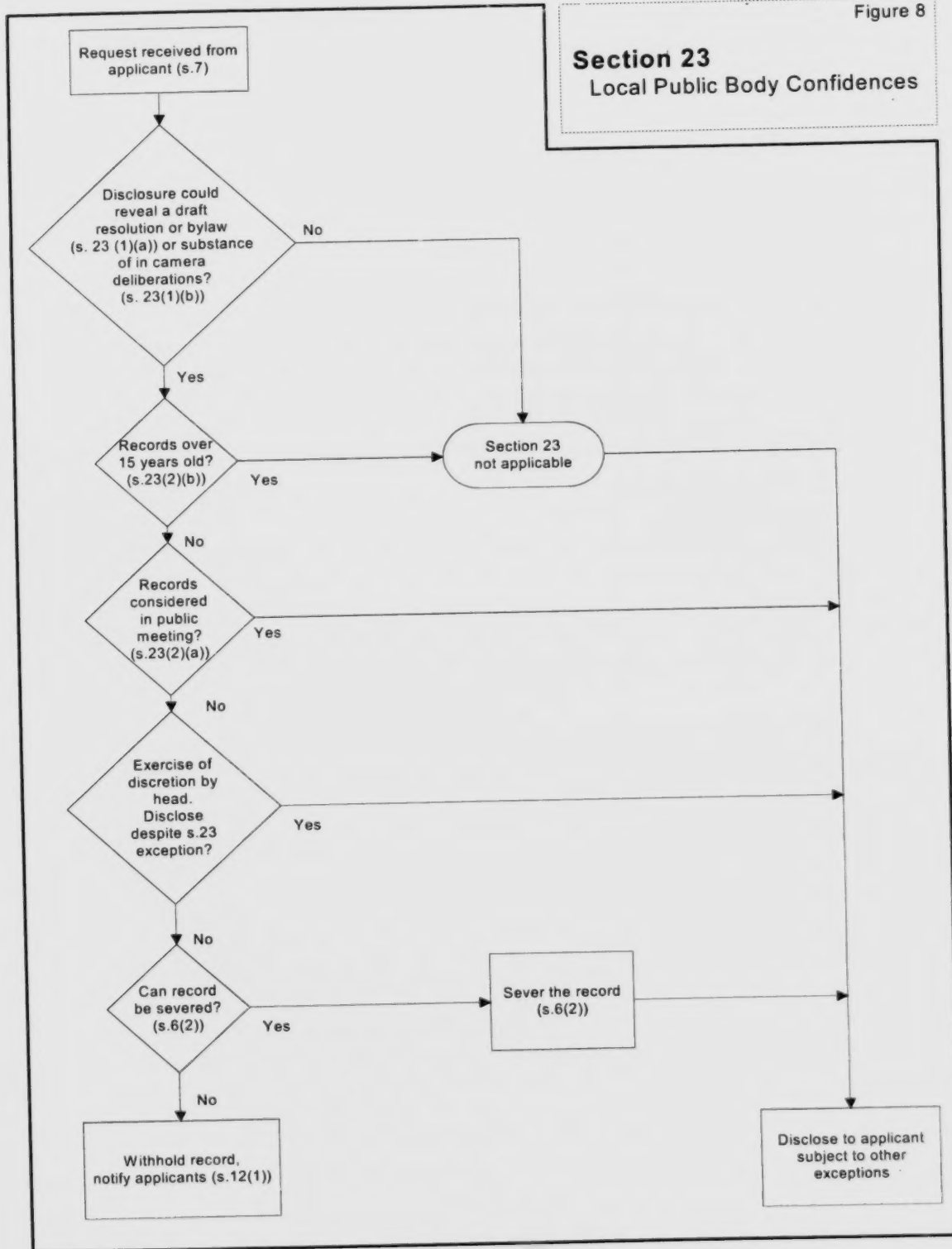
The exception cannot be applied to any information referred to in **section 23(1)(a)** and **(b)** if it is in a record that has been in existence for 15 years or more. See section 4.1 of this chapter for a discussion of the application of time limitations.

#### **Application of exception**

**Section 23** is applied in a series of steps that are outlined in the flowchart in Figure 8.

Figure 8

**Section 23**  
Local Public Body Confidences



#### 4.10 Advice from Officials

**Section 24(1)** is a discretionary exception that is intended to foster the candid exchange of views in the deliberative process involving senior officials and heads of public bodies, and their staff, as well as among officials themselves. This exception also protects the deliberative process involving senior officials of public bodies and the governing bodies of local public bodies.

This exception applies to information generated during the decision-making process, not to the decision itself (*IPC Order 96-012*).

**Section 24** was amended in 2006 by the addition of a mandatory exception for records in the custody of a public body that relate to an audit by the Chief Internal Auditor of Alberta (**section 24(2.1)**). This exception to disclosure is separate from the limited exclusion for audit records in the custody of the Chief Internal Auditor in **section 6(7)**.

#### **Classes of information to which section 24(1) may apply**

**Section 24(1)** provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to reveal

- advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council (**section 24(1)(a)**);
- consultations or deliberations involving
  - officers or employees of a public body,
  - a member of the Executive Council, or
  - the staff of a member of the Executive Council (**section 24(1)(b)**);
- positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of the Government of Alberta or a public body, or considerations that relate to those negotiations (**section 24(1)(c)**);
- plans relating to the management of personnel or the administration of a public body that have yet to be implemented (**section 24(1)(d)**);
- the contents of draft legislation, regulations and orders of members of the Executive Council or the Lieutenant Governor in Council (**section 24(1)(e)**);
- the contents of agendas or minutes of meetings of the governing body, or a committee of a governing body, of an agency, board, commission, corporation, office or other body that is designated as a public body in **Schedule 1** of the FOIP Regulation or in a FOIP (Ministerial) Regulation (**section 24(1)(f)**);
- information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision (**section 24(1)(g)**); or
- the contents of a formal research or audit report that is incomplete unless no progress has been made on the report for at least 3 years (**section 24(1)(h)**).

The exception is discretionary. Discretion needs to be exercised in determining whether or not disclosure of a particular record or part of a record could reasonably be expected to reveal particular information about either the process itself or the matters being discussed.



In determining whether or not to invoke the exception, public bodies should undertake a three-step process. They should

- determine whether the information requested falls within one of the classes of information to which the exception to disclosure may apply;
- if it does, then determine whether or not disclosure of the information could reasonably be expected to reveal the particular class of information involved; and
- exercise discretion as to whether or not to disclose the record or part of the record based on whether or not disclosure would affect deliberative processes in the future.

The exercise of discretion regarding this type of advisory information should be based on the impact the disclosure can reasonably be expected to have on the public body's ability to carry out similar internal decision-making processes in the future. Consideration should be given to whether disclosure of the information in this instance would

- make advice less candid and comprehensive;
- make consultations or deliberations less frank;
- hamper the policy-making process;
- have a negative effect on the ability of a public body or the government to develop and maintain strategies and tactics for present or future negotiations; or
- undermine the public body's ability to undertake personnel or administrative planning.

Such determinations can only be made on a case-by-case basis, bearing in mind the magnitude of the process involved, the procedures for decision-making that have been followed, and the sensitivity of the particular information. Public bodies should take into account the effect disclosure would have on all steps of a decision-making process and not just the immediate interests regarding the particular information in question.

Information about deliberative processes is revealed if the information makes direct reference to those processes, or if it allows an accurate inference to be made about those processes.

The Act sets out eight specific areas that allow for the possible non-disclosure of information. Each of these areas is discussed in detail below.

***Advice, proposals, recommendations, analyses or policy options***

**Section 24(1)(a)** This exception is intended to allow for candour during the policy-making process, rather than providing for the non-disclosure of all forms of advice (see *IPC Order 99-001*) or all records related to the advice (*IPC Order 99-040*).

This exception applies to these advisory functions at all levels in a public body. It also applies to advice and recommendations obtained from outside the public body, including advice and recommendations received under a contractual or other advisory arrangement (see *IPC Order F2005-012*). However, it does not apply to unsolicited documents sent to a public body by special interest groups for lobbying purposes (see

*IPC Order 2001-002*) or to records created by a third party participating in a general stakeholder consultation (see *IPC Orders F2004-021* and *F2008-008*).

The exception provides specific coverage for advice, proposals, recommendations, analyses, and policy options developed by or for a member of the Executive Council.

*Advice* includes the analysis of a situation or issue that may require action and the presentation of options for future action, but not the presentation of facts.

*Recommendations* includes suggestions for a course of action as well as the rationale for a suggested course of action.

*Proposals* and *analyses or policy options* are closely related to advice and recommendations and refer to the concise setting out of the advantages and disadvantages of particular courses of action.

The Information and Privacy Commissioner has defined all these terms as types of advice. The Commissioner's criteria for advice are that it should be

- sought or expected, or be part of the responsibility of a person by virtue of that person's position;
- directed towards taking an action, including making a decision; and
- made to someone who can take or implement the action.

See *IPC Orders 96-006* and *2001-002* for further explanation of the definition of advice.

The Commissioner has determined that a statement of fact that is not directed toward action to be taken does not qualify as advice under **section 24(1)(a)** (see *IPC Order 97-007*).

If the factual information is sufficiently interwoven with other advice that it cannot reasonably be considered separate or distinct, it may be withheld under this exception (see *IPC Order 99-001*).

**Section 24(1)(a)** would not normally apply to the details of a study or background paper where factual information is presented to describe certain issues, problems or events. Rather, it applies to the statements of advice or recommendations that set out or analyze possible directions or options in dealing with an issue or problem, to establish a policy or to make a decision.

For example, **section 24(1)(a)** could be applied to a report prepared by an investigation panel to advise a senior official on how to handle a complaint (see *IPC Orders F2003-014* and *F2003-016*).

There are cases where the disclosure of advice could reveal information that would cause damage to the internal decision-making processes of a public body. Disclosure could also affect the public body's overall ability to effectively manage programs and activities. At the same time, there are also cases where the disclosure of advice would have little or no effect on the overall administration or operation of the affected program or activity.

**Section 24(1)(a)** would not apply where the disclosure of information would not reasonably be expected to reveal advice or recommendations. For example, the disclosure of documents discussed at a meeting of a Cabinet Policy Committee that is open to the public would not *reveal* advice (see *IPC Order 2001-002*). The exception also would not apply to the names of correspondents, dates, subject lines that do not reveal advice, or information that reveals that a person participated in a discussion about a particular subject matter but does not indicate anything substantive about their involvement (*IPC Order F2004-026*).

***Consultations or deliberations***

**Section 24(1)(b)** This provision allows discretion to refuse access to those records or parts of records containing consultations or deliberations involving officers or employees of a public body, a minister or a minister's staff.

A *deliberation* for the purposes of this exception is a discussion of the reasons for and against a future action by an employee or officer of a public body (see *IPC Order 96-006*).

Deliberations include information indicating that a decision-maker relied on the knowledge or opinions of particular persons (see *IPC Order F2004-026*).

A *consultation* is a very similar activity where the views of one or more employees are sought about the appropriateness of a specific proposal or potential action (see *IPC Orders 96-006* and *F2003-016*).

Consultations include correspondence between third party advisors and government departments which was conveyed to the public body by a government department as background information to enable the public body to provide advice (e.g. when officials are asked to comment on advice already developed by other officials) (*IPC Order F2004-026*).

This discretionary exception is provided for the purpose of permitting the frank exchange of views among a number of individuals whose employment responsibilities include a consultative function. Within public bodies, consultations and deliberations are normally carried on in an organized manner through the exchange of hard copy memoranda and proposals and e-mail.

Agendas and minutes of meetings are also documents that may reveal consultations and deliberations. There is no blanket exception for such records, but consultative and deliberative material may be severed from these records.

**Section 24(1)(b)** covers consultations or deliberations at all levels in a public body and also those involving a minister or his or her staff.

The exception does not apply to records created and provided to the public body by a third party participating in a general stakeholder consultation. The third party is simply providing its own comments. This differs from the situation where a specific stakeholder, with particular knowledge, expertise or interest in a topic, has been asked to provide advice, recommendations or analysis (*IPC Orders F2004-021* and *F2008-008*).

The exception also will not apply to the names of correspondents, dates, subject lines that do not reveal advice, or information that reveals that a person participated in a discussion about a particular subject matter but does not indicate anything substantive about his or her involvement (*IPC Order F2004-026*).

***Positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations***

**Section 24(1)(c)** This provision covers the strategies, plans, approaches and bargaining positions that have been employed or are contemplated for the purposes of contractual and other negotiations. **Section 24(1)(c)** applies to individual public bodies and to the Government of Alberta as a whole. Access to such information can be refused even after particular negotiations have been completed.

*Positions and plans* refers to information that may be used in the course of negotiations.

*Procedures, criteria, instructions and considerations* are much broader in scope, covering information relating to the factors involved in developing a particular negotiating position or plan.

Examples of the type of information that could be covered by this exception are the various positions developed by government or local public body negotiators in relation to labour, financial and commercial contracts.

**Section 24(1)(c)** extends to situations where an agent retained for these purposes carries out negotiations on behalf of the government or a public body.

***Plans relating to the management of personnel or administration of the public body that have not yet been implemented***

**Section 24(1)(d)** This provision covers plans relating to the internal management of public bodies, including information about the relocation or reorganization of government departments and agencies, as well as reorganization within local public bodies.

The provision applies only within a limited time frame. Once a plan has been implemented, the information relating to it can no longer be withheld under this exception (see *IPC Order F2007-022*).

*Management of personnel* refers to all aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees (*IPC Investigation Report 2001-IR-006*). This includes staffing requirements, job classification, recruitment and selection, employee salary and benefits, hours and conditions of work, leave management, performance review, training, separation and layoff. For the Government of Alberta, the term includes the government-wide network managed through Corporate Human Resources. It also includes the management of personal service contracts (i.e. contracts of service) but not the management of consultant, professional or other independent contractor contracts (i.e. contracts for service).

*Administration of a public body* comprises all aspects of a public body's internal management, other than personnel management, that are necessary to support the

delivery of programs and services. Administration includes business planning, financial operations, and contract, property, information, and risk management.

*Implementation* means the point when the implementation of a decision begins. For example, if a public body decides to go forward with an internal budget cut or restructuring of departments, implementation commences when this plan of action is communicated to its organizational units.

Although a final plan that has been implemented cannot be withheld under this exception, the options that were considered before deciding on the plan need not be disclosed. Plans that were never implemented can be withheld for 15 years (**section 24(2)(a)**). A public body may decide to withhold plans that were not implemented if, for example, there is reason to believe that injury or harm to the efficiency of the operation of the public body could reasonably be expected to result from disclosure.

#### ***Contents of draft legislation, regulations and orders***

**Section 24(1)(e)** This provision covers bills, regulations and orders of members of the Executive Council or the Lieutenant Governor in Council while they are being drafted and formulated in preparation for introduction to the Legislature, for publication or for public consultation. This provision covers all the drafts and not just the final draft of legislation, regulations and ministerial orders.

**Section 24(1)(e)** will not apply if disclosing the information would not reveal the substantive contents of the draft legislation. For example, in *IPC Order F2004-026*, **section 24(1)(e)** did not apply to the names of the individuals who prepared or commented on the legislation, the dates of the drafts and comments or several headings and subject-lines in communications about the drafts.

For draft bylaws and other legal instruments of local public bodies, see section 4.9 of this chapter.

#### ***Contents of agendas or minutes of meetings of the governing body of a designated public body***

**Section 24(1)(f)** This exception applies only to those public bodies listed in **Schedule 1** of the FOIP Regulation or designated as a public body by a FOIP (Ministerial) Regulation.

**Section 24(1)(f)** allows a public body to withhold agendas and minutes of meetings because the meetings to which they relate provide the focus for decision-making within these types of bodies. The exception can be applied only to the records of the governing body or a committee of the governing body of the public body.

**Section 24(1)(f)** covers only agendas and minutes of meetings, and not the background reports or studies used in a meeting. Background information cannot be withheld under this exception.

#### ***Pending policy and budgetary decisions***

**Section 24(1)(g)** This provision covers information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision. **Section 24(1)(g)** allows public



bodies to prevent premature disclosure of a policy or budgetary decision (see, for example, *IPC Order F2005-004*).

Once a policy or budgetary decision has been taken and is being implemented, the information can no longer be withheld under this exception. A decision is being implemented once those expected to carry out the activity have been authorized and instructed to do so.

***Formal research or audit reports that are incomplete***

**Section 24(1)(h)** This provision covers the contents of formal research and audit reports that, in the opinion of the head of the public body, are incomplete. The exception allows public bodies to withhold, for a limited period, information that could be misleading, inaccurate or incomplete.

*A formal research or audit report* is one that has been compiled in accordance with procedures intended to ensure the validity of the research or audit process. The research or audit is carried out in accordance with a recognized methodology.

*Audit* is defined as a financial or other formal and systematic examination or review of a program, portion of a program or activity (**section 24(3)**).

*Incomplete* means that the report is in preliminary or draft format, or is under review for consistency with the terms of reference for the report or for accuracy or completeness.

For this exception to apply, there should be some evidence that the research or audit report has not been finalized. For example, if a consultant's research report had been accepted by a public body and payment made in full without any indication that the report had not fulfilled the requirements of the contract, the report would probably be complete. A report submitted by an auditor to officials of a public body for review and discussion prior to its formal presentation would be incomplete.

**Section 24(1)(h)** applies only within a limited time frame. Once the report is accepted as complete, it cannot be withheld under this exception. If the report is submitted but no further progress is made on it for a period of 3 years, it cannot be withheld under this exception.

*Progress* implies some activity designed to finalize or complete the report, not simply a review of its contents with no subsequent action.

**When the exception does not apply**

**Section 24(2)** provides some specific cases where the exception in **section 24(1)** does not apply.

***Information in existence 15 years or more***

**Section 24(2)(a)** Any information contained within a record which has been in existence for 15 years or more cannot be withheld under **section 24(1)**. See section 4.1 of this chapter for a discussion of the application of time limitations. Other exceptions may still apply to the information.

**Statements of the reasons for decisions made in the exercise of a discretionary power or an adjudicative function**

**Section 24(2)(b)** This provision makes it clear that **section 24(1)** cannot be used to withhold formal judgments, including the reasons for reaching those judgments. The provision applies when the decision has already been made and is not merely contemplated.

*Reasons for decision* mean the motive, rationale, justification or facts leading to a decision.

*Exercise of discretionary power* refers to making a decision that cannot be determined to be right or wrong in an objective sense.

*Adjudicative function* means a function conferred upon an administrative tribunal, board or other non-judicial body or individual that has the power to hear and rule on issues involving the rights of people and organizations. Examples would be a school board hearing an appeal under the *School Act*, or a hearing by an assessment review board.

Reasons for decisions of this type cannot be withheld under **section 24(1)** despite the fact that the decisions may contain advice or recommendations prepared by or for a minister or a public body.

**Results of product or environmental testing**

**Section 24(2)(c)** This provision limits the scope of **section 24(1)** by excluding the results of product or environmental testing carried out by or for a public body from the exception to disclosure. In order for **section 24(2)(c)** to apply, the testing has to be complete or have had no progress made on it for at least 3 years.

Examples of the test results contemplated by **section 24(2)(c)** would information on products such as air filters or the results of environmental testing at a landfill or testing of a building's air quality.

**Section 24(2)(c)** does not apply to testing done

- for a fee as a service to a person other than a public body; or
- for the purpose of developing methods of testing or testing products for possible purchase.

Examples of test results to which **section 24(1)** therefore may apply, are the results of commercial product testing and soil testing. **Section 24(1)** may also apply if the testing was done for the purpose of developing methods of testing, for example, the development of a new methodology for recycling tires. There would have to be evidence in such cases that methodology development was the sole purpose of the testing.

**Section 24(1)** also covers test results where testing was done by a public body in order to determine whether or not to purchase a product.

**Statistical surveys**

**Section 24(2)(d)** This provision limits the scope of **section 24(1)** by excluding statistical surveys from the exception to disclosure.

*Statistics* is the science of collecting and analyzing numerical data and the systematic presentation of such facts.

*Statistical surveys* are general views or considerations of subjects using numerical data.

Where statistical surveys appear with information that can be withheld under **section 24(1)**, the excepted information should be severed and the statistical survey disclosed.

An example of a statistical survey would be a study of growth rates in various forested areas of northern Alberta. Such a study could not be withheld under **section 24(1)** even though it may be part of a larger document dealing with reform of forestry law, regulation or policy.

**Results of background scientific or technical research in connection with the formulation of a policy proposal**

**Section 24(2)(e)** This provision limits the scope of **section 24(1)** by excluding from the exception to disclosure background research undertaken as the basis of formulating a policy proposal.

*Background research* encompasses a wide range of study, review and fieldwork aimed at analyzing and presenting an overview of issues.

For this provision to apply, the research has to be completed or have had no progress made on it for at least 3 years.

**Section 24(2)(e)** applies to research that is scientific (conducted according to the principles of objective research) or technical (based on a particular technique or craft) and directed toward policy formulation. In order for information to be considered background research under this provision, it must be connected with the development of some specific policy. This would clearly be the case if, for example, a policy proposal referred directly to the research on which the proposal was based.

Normally the research methodology, data and analysis cannot be withheld under **section 24(1)**. However, advice and recommendations contained in the same record as the background research or prepared separately by or for a public body or a minister could be withheld.

**Instructions or guidelines issued to public body officers or employees**

**Section 24(2)(f)** This provision limits the scope of **section 24(1)** by excluding from the exception to disclosure information used by officials in interpreting legislation, regulations or policy. **Section 24(2)(f)** also excludes information used by officials in exercising the discretion given to them under an Act of the Legislature or a bylaw of a local public body.

Generally, an official or employee in a position to provide interpretation or policy direction will have issued the instruction or guideline.

**Substantive rule or policy statement used to interpret legislation or administer a public body program or activity**

**Section 24(2)(g)** This provision expands on **section 24(2)(f)**. It excludes from the scope of **section 24(1)** the basic interpretations of the law, regulations and policy under which a public body operates its programs and activities.

This provision complements **section 89(1)** of the Act, which requires that public bodies have in place facilities to enable the public to examine any manual, handbook or other guideline used in decision-making processes that affect the public.

**Records relating to an audit by the Chief Internal Auditor of Alberta**

**Section 24(2.1)** **Section 24(2.1)** creates a mandatory exception to disclosure for records and information relating to an audit by the Chief Internal Auditor of Alberta.

The Chief Internal Auditor of Alberta provides independent, objective assurance and advisory services to government departments to improve the effectiveness, efficiency and economy of government operations.

**Section 24(2.1)(a)** requires a public body to refuse to disclose records relating to a audit that are *created by or for* the Chief Internal Auditor. This would include any record that was provided to the public body by the Chief Internal Auditor relating to an audit, including correspondence, meeting notes, reports and management letters relating to the audit. Because the records must be created by or on behalf of the Chief Internal Auditor, **section 24(2.1)(a)** would not apply to records created by the public body at the request of the Chief Internal Auditor.

**Section 24(2.1)(b)** requires a public body to refuse to disclose information that would *reveal information about* an audit by the Chief Internal Auditor. Program records that were considered in the course of an internal audit or records that were compiled for the Chief Internal Auditor would not fall within this provision unless the records themselves reveal information about the audit.

**Section 24(2.2)** The exception in **section 24(2.1)** does not apply

- if 15 years or more has elapsed since the audit to which the record relates was completed (**section 24(2.2)(a)**), or
- if the audit to which the record relates was discontinued or if no progress has been made on the audit for 15 years or more (**section 24(2.2)(b)**).

These time limitations on the exception are the same as those for the exclusion in **section 6(8)**.

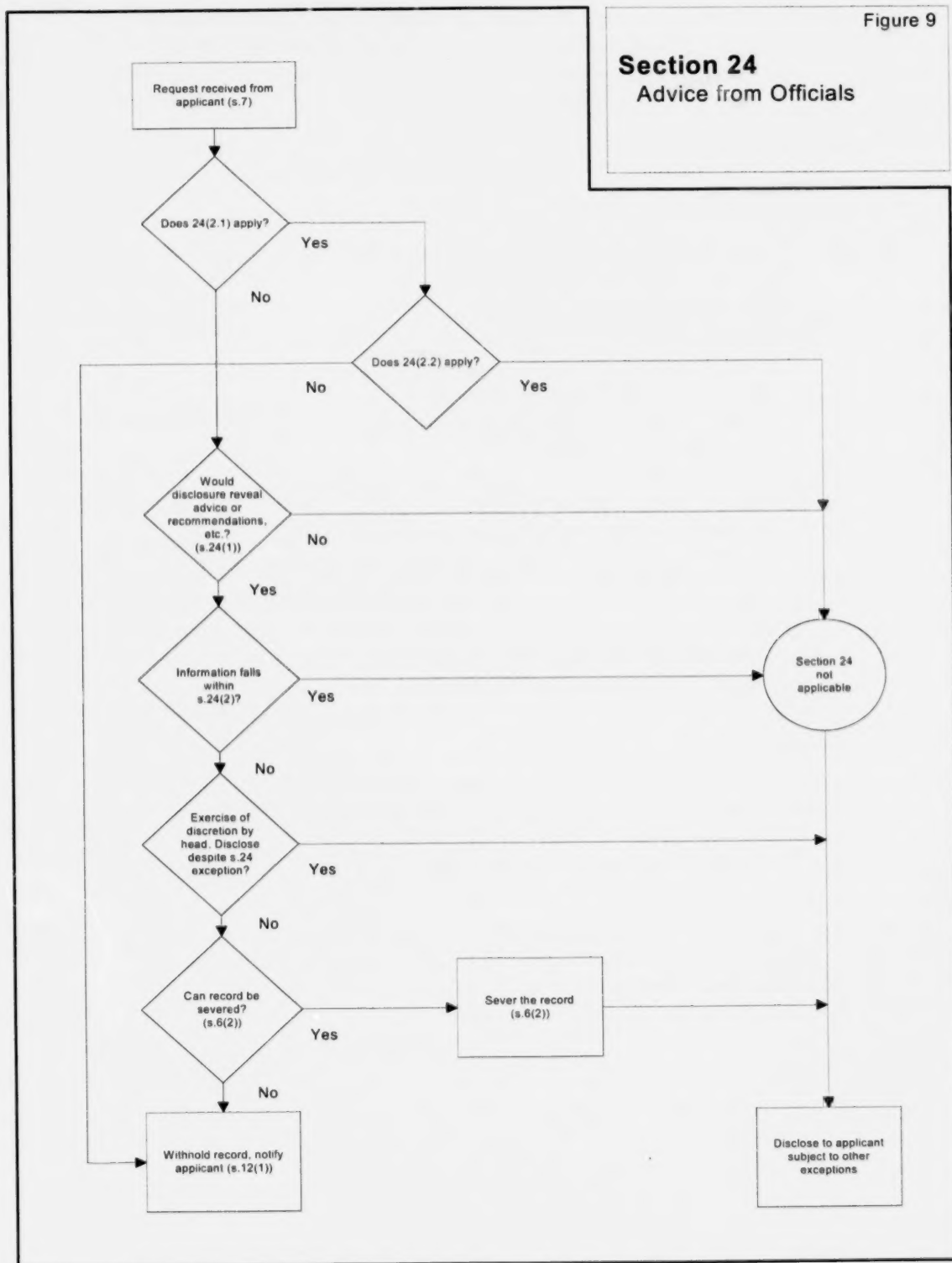
**Application of exceptions**

Figure 9 contains a flowchart setting out the steps for applying **section 24**.

Figure 9

## Section 24

### Advice from Officials





**4.11  
Disclosure  
Harmful to  
Economic and  
Other Interests  
of a Public  
Body**

**Section 25(1)** of the Act provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to harm the economic interest of a public body or the Government of Alberta as a whole, or the ability of the Government to manage the economy (see e.g. *IPC Orders 96-012* and *96-013*).

**Section 25** is a discretionary exception. The information that can be withheld under this exception includes

- trade secrets of a public body or the Government of Alberta (**section 25(1)(a)**);
- financial, commercial, scientific, technical or other information in which a public body or the Government of Alberta has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value (**section 25(1)(b)**);
- information the disclosure of which could reasonably be expected to
  - result in financial loss to,
  - prejudice the competitive position of, or
  - interfere with contractual or other negotiations of the Government of Alberta or a public body (**section 25(1)(c)**); and
- information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee or the public body of priority of publication (**section 25(1)(d)**).

The exception refers to the Government of Alberta as a whole. This recognizes that public bodies, individually or collectively, may hold significant amounts of financial and economic information that is critical to the management of the provincial economy. **Section 25(1)** ensures that, where harm would result from disclosure of information, the information may be withheld.

**Harms test**

In order to use the exception, a public body must have objective grounds for believing that disclosure will likely result in harm. In order to determine whether there is a reasonable expectation of harm, the test established in *IPC Order 96-003* must be satisfied. This test is discussed in the introduction to this chapter (section 4.1).

The context in which a public body operates should be taken into account in determining whether it is reasonable to expect that harm will result from the disclosure of the information. In applying this exception, public bodies should take into account not just the specific harm that could occur as a result of disclosure of the information (i.e. **section 25(1)(a) to (d)**) but also whether the broader economic interests of the public body or the Government of Alberta would be harmed.

*Economic interests* refers to both the broad interests of a public body and, for provincial public bodies, of the government as a whole, in managing the production, distribution and consumption of goods and services. The term also covers financial matters such as the management of assets and liabilities by a public body and the public body's ability to protect its own or the government's interests in financial transactions.

The *financial interests* of the Government of Alberta include the ability to collect taxes and generate revenues.

Harm to these interests includes damage or detriment to the economic policies or activities for which a single public body is responsible, as well as harm to policies and programs that affect the overall economy of the province. Harm to these interests also includes monetary loss or loss of assets with monetary value.

Examples of information to which the exception in **section 25** may apply include

- information on a public body's investment strategies which could affect its interests or future financial position;
- information in budget preparation documents which could result in segments of the private sector taking actions affecting the ability of the government or a local public body to meet economic goals;
- information about licensing and inspection practices of a public body which could affect the amount of revenue collected; and
- information about a trade deal, a development plan or strategy or an economic negotiation that has not been completed.

**Section 25(1)** does not prevent the release of information that reveals a liability that might lead to a lawsuit against a public body for alleged wrongdoing.

In most cases, the public body whose economic interests are involved will be the public body with custody or control of the record(s) requested. In some instances, however, a public body may hold information about another public body whose economic interests may be affected by disclosure. Consultation is essential between the two bodies in such situations when use of **section 25(1)** is being considered.

The exception may also be claimed for the Government of Alberta in the broad, corporate sense. The term Government of Alberta has a broader sense here than an individual government department or agency.

The phrase *ability to manage the economy* refers to the responsibility of the Government of Alberta to manage the province's economic activities by ensuring that an appropriate economic infrastructure is in place, and by facilitating and regulating the activities of the marketplace. This depends on a range of activities, including fiscal and economic policies, taxation, and economic and business development initiatives.

### **Types of information**

The types of information listed in **section 25(1)** are illustrative only and may not cover all types of information, which, if disclosed, could reasonably be expected to cause harm to economic interests. At the same time, inclusion in one of the categories in **section 25(1)** is not by itself sufficient to allow a public body to refuse access. Application of this exception is subject to the harms test.



A public body must have reasonable grounds to expect harm as a result of disclosure in order to apply the exception.

### **Trade secrets**

**Section 25(1)(a)** *Trade secret* is defined in **section 1(s)** of the Act as meaning information, including a formula, pattern, compilation, program, device, product, method, technique or process

- that is used, or may be used, in business or for any commercial purpose;
- that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use;
- that is the subject of reasonable efforts to prevent it from becoming generally known; and
- the disclosure of which would result in significant harm or undue financial loss or gain.

Information must meet all of these criteria to be considered a trade secret.

Information that is generally available through public sources (e.g. published research reports) would not usually qualify as a trade secret under the Act.

A public body must own the trade secrets or must be able to prove a claim of legal right in the information (e.g. a licence agreement) in order to apply the exception. Normally, this will mean that the trade-secret information has been created by employees of the public body as part of their jobs, or by a contractor as part of a contract with the public body.

For example, software developed by a public body or special testing equipment which has been kept secret or confidential would have economic value. Disclosure of the specifications could reasonably be expected to result in improper benefit and the information could probably qualify as a trade secret. On the other hand, details of a minor technical adjustment to equipment that has been inspired by an article in a trade journal would not be withheld under this exception.

**Section 25(1)(a)** does not apply to trade secrets of a third party. Requirements relating to the protection of these trade secrets are dealt with in **section 16(1)(a)**. See section 4.2 of this chapter.

### **Financial, commercial, scientific, technical or other information where there is a proprietary interest**

**Section 25(1)(b)** The exception in this provision is subject to a three-part test. In order for the exception to apply, all of the following conditions must be met:

- the information must be financial, commercial, scientific, technical or other information;
- the public body or the Government of Alberta must have a proprietary interest or a right of use; and

- the information must have, or be reasonably likely to have, monetary value.

The following definitions have been taken from IPC Orders dealing with **section 16**.

*Commercial information* means information relating to the buying, selling or exchange of merchandise or services. This includes third party associations, past history, references and insurance policies (see *IPC Order 98-006*) and pricing structures, market research, business plans, and customer records (see *IPC Order 96-013*). To determine whether the information in question is commercial information, the record needs to be viewed as a whole (see *IPC Order 98-006*). An agreement between two business entities may contain commercial information (see *IPC Order 2001-019*).

*Financial information* is information regarding the monetary resources of a third party, such as the third party's financial capabilities, and assets and liabilities, past or present (see *IPC Orders 96-018* and *2001-008*). Common examples are financial forecasts, investment strategies, budgets, and profit and loss statements (see *IPC Order 96-013*).

*Scientific information* is information exhibiting the principles or methods of science (see *IPC Order 2000-017*). The information could include designs for a product and testing procedures or methodologies.

*Technical information* is information relating to a particular subject, craft or technique (see *IPC Order 2000-017*). Examples are system design specifications and the plans for an engineering project.

The second part of the test for this exception requires that the public body or the Government of Alberta have a *proprietary interest* in the information. This means that the public body or the government must be able to demonstrate rights to the information. For example, a municipality may have a proprietary interest in geographical information systems mapping data or statistical data.

The third part of the test is whether the information has or is reasonably likely to have monetary value. *Monetary value* may be demonstrated by evidence of potential for financial return to the public body or government. An example of information that is reasonably likely to have monetary value might include a course developed by a teacher employed by a school board.

***Financial loss, prejudice to competitive position, or interference with negotiations***

**Section 25(1)(c)** This exception applies to information the disclosure of which could reasonably be expected to result in financial loss to, prejudice the competitive position of, or interfere with contractual or other negotiations of the Government of Alberta or a public body.

**Section 25(1)(c)** provides similar protection for business enterprises in the public sector as is provided for private sector third parties under **section 16(1)(c)**. To claim the exception, a public body must have objective grounds for believing that one of the harms listed will result from disclosure.

In the case of *financial loss*, there must be reasonable grounds to believe that disclosure of information in the specific record would result in direct monetary or equivalent loss. This includes loss of revenue, loss of reputation or loss of good will in the marketplace. The loss cannot be speculative nor can it be loss expected as a result of a “ripple effect” (see *IPC Order 98-020*).

In the case of *prejudice to competitive position*, a public body must have a reasonable expectation that disclosure of the information is capable of being used by an existing or potential competitor to reduce the public body’s or the government’s share of a market. The exception may be claimed whether or not there is currently a competitor in the marketplace (*IPC Order 97-005*).

*Interfere with contractual or other negotiations* means to obstruct or make much more difficult the negotiation of a contract or other sort of agreement between the public body or the government and a third party. The expectation of interference with negotiations as a result of disclosure must be reasonable and the negotiations have to be specific, not simply possible negotiations of a general kind in the future (see *IPC Order 98-005*).

Examples of where **section 25(1)(c)** has been found to not apply include the following.

- Disclosure of the hourly rate of, and hours worked by, fee-for-service instructors of a post-secondary institution. There was no risk of economic harm to the institution since the applicant (the academic faculty association) was bound by a confidentiality clause to not distribute the information to other institutions or instructors (*IPC Order F2004-014*).
- Disclosure of the salary and benefits set out in an employment contract of a senior official. The disclosure of the specific information would not, in itself, harm the ability of the Government or the public body to negotiate future contracts since any job candidate could develop a negotiating strategy from the salary and benefits information available in ministry annual reports (*IPC Orders F2006-007 and F2006-008*).
- Disclosure of the number, types and outstanding amounts of student loans sold to a collection agency, which would only give the applicant general information (*IPC Order 2000-009*).

The following are examples of where **section 25(1)(c)** has applied.

- Disclosure of unpublished information about required and recommended course books of post-secondary institutions to an applicant who intended to open a used book store. The disclosure would negatively impact the sale of used books by the institutions (*IPC Order F2006-023*).
- Disclosure of records relating to a post-secondary institution’s fund-raising activities, which would damage its relationship with private-sector participants and prejudice its position in existing and future revenue-generating projects (*IPC Order F2004-012*).



**Research information where employee or public body could be deprived of priority of publication**

**Section 25(1)(d)** Public bodies employ a wide range of researchers, including professional scientists, technicians and social scientists. Their reputations are often dependent on the research they publish.

The fact that the employees have a professional reputation is of considerable value to public bodies that employ them. In addition, their research often has monetary and program value for the public bodies. For these reasons, the Act protects the priority of publication for all types of research.

Examples include scientific and technical research carried out at research institutes or universities; historical research connected with the designation or preservation of historical or archaeological resources; and epidemiological and other medical studies carried out in health care bodies. A public body would have to be able to provide some proof that publication is expected to result from the research or that similar research in the past has resulted in publication.

**When the exception does not apply**

**Section 25(2)** provides that a public body must not refuse to disclose under **section 25(1)** the results of product or environmental testing carried out by or for a public body, unless the testing was done

- for a fee as a service to a person, other than the public body (**section 25(2)(a)**); or
- for the purpose of developing methods of testing or testing products for possible purchase (**section 25(2)(b)**).

The intent of the provision is to ensure that a public body does not withhold information resulting from product or environmental testing carried out either by the employees of a public body or on its behalf by another organization. Examples include information on products such as air filters, environmental test results on water quality or air quality and commercial product testing and soil testing.

Information can be withheld when the public body performs the testing, for a fee, as a service to a private citizen or private corporate body.

The information may also be withheld if the testing was done for the purpose of developing testing methods, such as a new methodology for tire recycling. There would have to be evidence in such cases that methodology development was the sole purpose of the testing.

The exception can also be used to withhold test results compiled to determine whether or not a public body would purchase a product.

In all three circumstances, the harms test in **section 25(1)** still has to be met before the information can be withheld.

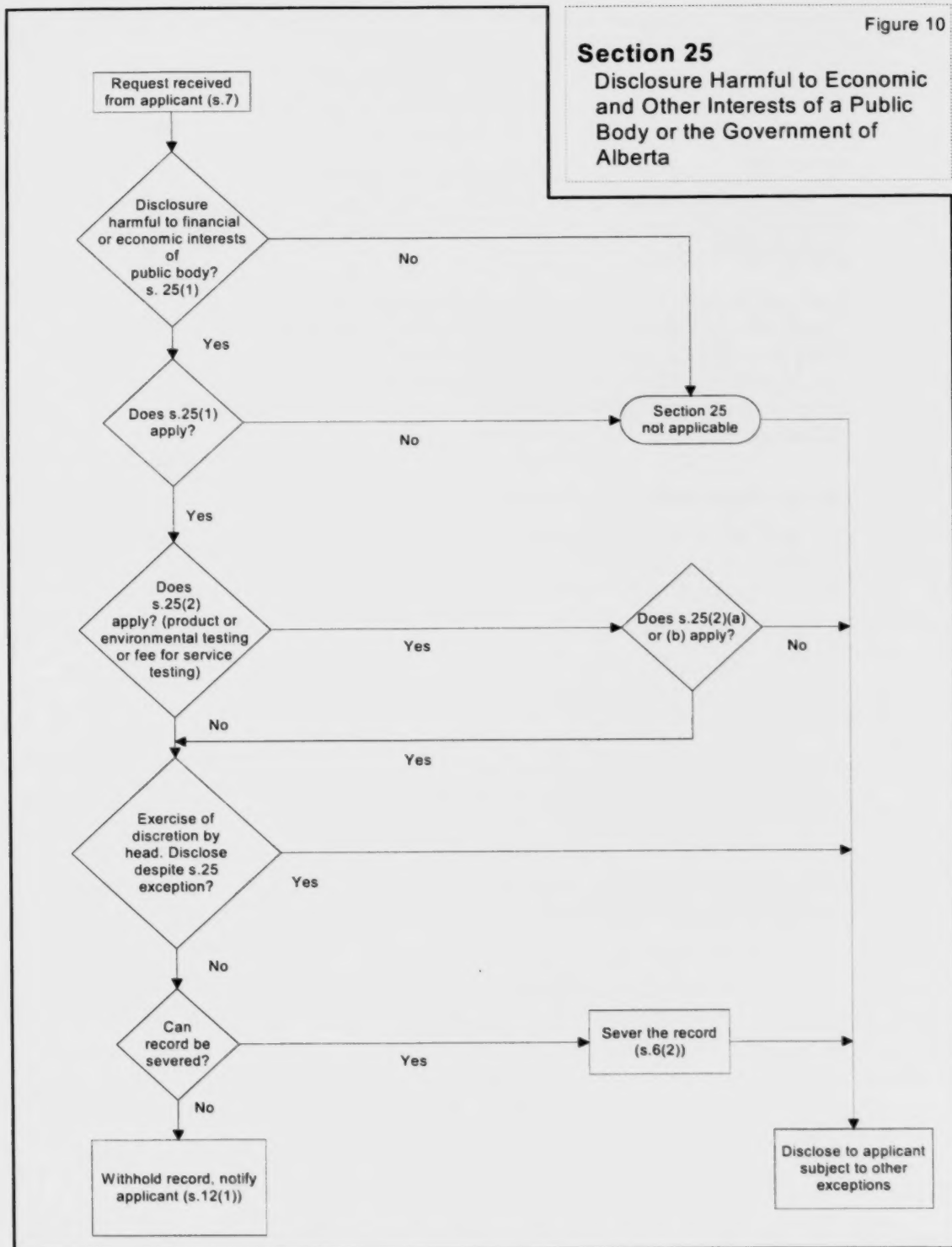
**Applying the exception**

Figure 10 contains a flowchart setting out the steps for applying **section 25**.

Figure 10

**Section 25**

Disclosure Harmful to Economic  
and Other Interests of a Public  
Body or the Government of  
Alberta



#### 4.12 Testing Procedures

**Section 26** of the Act provides that a public body may refuse to disclose information relating to

- testing or auditing procedures or techniques (**section 26(a)**);
- details of specific tests to be given or audits to be conducted (**section 26(b)**); or
- standardized tests used by a public body, including intelligence tests (**section 26(c)**).

The exception applies only if the disclosure could reasonably be expected to prejudice the use or results of particular tests or audits.

**Section 26** is a discretionary exception.

This exception provides protection for the procedures and techniques involved in testing and auditing. It also protects details relating to specific tests to be given or audits to be conducted.

The terms *test* and *audit* cover a wide range of activities. Examples include environmental testing, staffing examinations, personnel audits, financial audits, and program audits. Specific mention is made in **section 26(c)** of standardized tests, such as intelligence tests. Other standardized tests include psychological tests and aptitude tests, which are often used in educational bodies.

The exception may be applied where disclosure of a specific test to be given or audit to be conducted, or one that is currently in process, would invalidate the results. This applies even if there is no intention to use the test or audit again in the future.

The exception may also apply where there is an intention to use the testing or auditing procedure in the future, and disclosure would result in unreliable results being obtained and the test or audit having to be abandoned as a result. Test questions that are regularly used – for example, in making staffing decisions – may be excepted from disclosure.

For example, **section 26** was found to apply to standardized interview questions, evaluation keys and an essay written by the applicant because their disclosure could prejudice the utility of such tests in future police recruitment processes (*IPC Order F2004-022*).

Information relating to a test or an audit that has been used in the past, but which is neither in process nor to be used in the future, cannot be withheld under this exception.

**Section 26** does not allow public bodies to withhold the results of tests or audits, including the results of standardized tests. Public bodies should consider in advance how they will handle issues that might arise from the disclosure of test results that contain sensitive information or would likely be open to misinterpretation by a non-expert.

**4.13  
Privileged  
Information**

**Section 27** of the Act is an exception to disclosure of information that allows a public body to withhold information that is subject to a legal privilege, or relates to the provision of legal services or the provision of advice or other services by the Minister of Justice and Attorney General or a lawyer.

**Section 27(1)** provides that a public body may refuse to disclose information that

- is subject to any type of legal privilege, including solicitor–client privilege and parliamentary privilege;
- relates to the provision of legal services and is prepared by or for specified individuals; or
- relates to the provision of advice or other services contained in correspondence between specified individuals.

**Section 27(2)** requires that a public body refuse to disclose information that is subject to a legal privilege where that information relates to a person other than the public body.

**Section 27(3)** states that only the Speaker of the Legislative Assembly may determine whether information is subject to parliamentary privilege.

The intent of **section 27** is to ensure that information privileged at law, as well as other similar information in the custody or under the control of a public body, is protected from disclosure in much the same way as an individual's information would be by his or her own lawyer.

**Indicators**

The following is a non-exclusive list of indicators that, if present, suggest that **section 27** might apply:

- the record is a letter, fax, e-mail or other correspondence to or from the public body's lawyer, including a lawyer at Alberta Justice and Attorney General (for government departments and agencies);
- the record is attached to correspondence to or from a lawyer;
- the record is a lawyer's briefing note or working paper;
- the record is a communication between employees of a public body, or between employees of a third party, quoting legal advice given by a lawyer;
- the record is a note documenting legal advice given by a lawyer or a statement of account from a lawyer that details the services provided by the lawyer;
- the information was provided by a confidential informant;
- the information relates to an existing or contemplated lawsuit;
- the information relates to a criminal prosecution;
- the information is contained in correspondence to or from the Minister of Justice and Attorney General or correspondence to or from an agent of the Minister of Justice and Attorney General;
- the record relates to a public body's investigation of a third party; or
- the record relates to the operations of the Legislative Assembly.



If one or more of these indicators exist, **section 27** may apply. Public bodies should consider consulting with legal counsel when a record contains information that may qualify for exception under **section 27** and the public body is unsure whether to claim its legal privilege. The first step is to determine whether legal privilege applies. The next step is to decide whether the privilege should be waived.

## Privileged information

### Legal privilege

**Section 27(1)(a)** **Section 27(1)(a)** gives a public body the discretion to refuse to disclose information that is subject to any type of legal privilege. There are several types of legal privilege. They include

- solicitor–client privilege;
- litigation privilege;
- common interest privilege;
- parliamentary privilege;
- police informer privilege;
- case-by-case privilege for private records and for Crown records;
- settlement negotiation privilege; and
- statutory privilege.

If one of these privileges applies, the information may be withheld under **section 27(1)(a)**.

Public bodies should note that, since **section 27(1)(a)** is a discretionary exception, the Information and Privacy Commissioner will not raise it as an exception to disclosure if the public body does not.

**Solicitor–client privilege.** This privilege applies to a record when

- the record is a communication between a lawyer and the lawyer’s client;
- the communication entails the seeking or giving of legal advice; and
- the record is intended to be confidential by the parties (see *IPC Orders 96-017* and *96-021*).

*Legal advice* means a legal opinion about a legal issue, and a recommended course of action, based on legal considerations, regarding a matter with legal implications (see *IPC Order 96-017*).

In *IPC Order 96-020*, the Commissioner said that solicitor–client privilege will apply to a continuum of communications or legal advice, including not only telling the client the law, but also giving advice as to what should be done in the relevant legal context. The facts of each case will be important to determine what functions performed by a lawyer for his or her client would fall within the continuum of legal advice.



Solicitor–client privilege applies to attachments to communications between a solicitor and his or her client when the attachments are part of the continuum of the legal advice (see *IPC Orders 98-004* and *99-005*).

In order to apply solicitor–client privilege, the public body must be able to provide evidence of the confidential legal advice sought or given and evidence of who sought the advice or to whom it was given (see *IPC Order 2000-019*).

The presence of an agent does not destroy solicitor–client privilege, as long as the communication through the agent meets the test for solicitor–client privilege (see *IPC Order 97-003*).

Lawyers' bills of accounts are presumed to be subject to solicitor–client privilege. However, the presumption can be rebutted by showing that there is no reasonable possibility that an inquirer, aware of background information available to the public, could use the information about the amount of fees paid to deduce or acquire any communication protected by solicitor–client privilege.

In *IPC Order F2007-014*, it was found that disclosure of the total amount of the bill, the law firm's letterhead and the name and address of the client would not reveal privileged communications. In *IPC Order F2007-025*, solicitor–client privilege applied to the date the legal service was provided, the description of the service provided, the breakdown of the fees and the identity of the lawyer providing the service. However, the total amount of the bill and the letterhead of the law firm could be disclosed.

The Commissioner has established a protocol as to how records for which solicitor–client privilege has been claimed will be dealt with during a review. The *Solicitor–Client Privilege Adjudication Protocol* is available on the Commissioner's website.

**Litigation privilege.** This privilege applies to records created or obtained by a client for the use of the client's lawyer in existing or contemplated litigation. Litigation privilege also applies to records created by a third party, or obtained from a third party on behalf of the client, for the use of the client's lawyer in existing or contemplated litigation.

To apply litigation privilege a public body must show that

- there is a third party communication, which may include
  - communications between the client (or the client's agents) and third parties for the purpose of obtaining information to be given to the client's lawyer to obtain legal advice,
  - communications between the solicitor (or the solicitor's agents) and third parties to assist with the giving of legal advice, or
  - communications which are created at their inception by the client, including reports, schedules, briefs, documentation, etc.;
- the maker of the record or the person under whose authority the record was made intended the record to be confidential; and

- the “dominant purpose” for which the record was prepared was to submit it to a legal advisor for advice and use in litigation. The “dominant purpose” test consists of three requirements:
  - the documents must have been produced with existing or contemplated litigation in mind;
  - the documents must have been produced for the dominant purpose of existing or contemplated litigation; and
  - if litigation is contemplated, the prospect of litigation must be reasonable (see *IPC Orders 97-009 and F2003-005*).

Litigation privilege will not apply if the records in question do not involve correspondence with a solicitor or show any intention to obtain legal advice (see *IPC Order 2001-018*).

Litigation privilege no longer applies once litigation has been concluded (see *IPC Orders 98-017 and 2001-025*). However, solicitor–client privilege may continue to apply to some of the records.

**Common interest privilege.** This privilege exists when records are provided among parties where several parties have a common interest in anticipated litigation. The privilege exists when one party consults with a lawyer on an issue of common interest and shares or exchanges the legal opinion with other parties with the same interest (see *IPC Orders 97-009 and 2001-018*).

**Parliamentary privilege.** This is a unique class privilege that extends to members of the Legislative Assembly immunity to do their legislative work.

**Section 27(3)** requires that the Speaker of the Legislative Assembly determine whether information is subject to this privilege.



**When a public body believes that all or part of a requested record may be subject to parliamentary privilege, it must provide notice to the Speaker of the Legislative Assembly. The notice must include a description of the contents of the record and a request that the Speaker determine whether or not parliamentary privilege applies to some or all of the information. The decision of the Speaker must be followed.**

**Model Letter K** in Appendix 3 may be used to request a determination from the Speaker. The Commissioner has said that if the Speaker decides that parliamentary privilege applies to a record, the Commissioner cannot review a public body’s decision to withhold that record. (See **section 65(5)(b)** of the Act and *IPC Order 97-017*.)

**Police informer privilege.** This privilege, also referred to as confidential informant privilege, applies to information that might identify an informer. The privilege protects individuals who choose to act as confidential informants from the possibility of retribution. This protection in turn encourages others to divulge pertinent

information to authorities. (See *IPC Order 96-020* for a discussion of the *R. v. Leipert* case, in which the Supreme Court of Canada affirmed that “informer privilege” is a legal privilege).

This privilege is subject to only one exception: “innocence at stake.” To raise this exception, there must be a basis on the evidence for concluding that disclosure of the informer’s identity is necessary to demonstrate the innocence of someone in a criminal proceeding.

**Case-by-case privilege.** This is a privilege that is found to exist for information in a particular case. In each case, the decision-maker must determine whether the public interest favours disclosure or non-disclosure of the record (see *IPC Order 96-020*).

**Case-by-case privilege applied to Crown records (sometimes called Crown privilege).** These records contain information relating to government activities or operations, and decisions at the highest level of government, such as Cabinet decisions concerning national security. In order to establish that a case-by-case privilege for Crown records exists, a public body must base an argument for public interest immunity on the following criteria:

- the nature of the policy concerned;
- the particular contents of the records;
- the level of the decision-making process;
- the time when a record or information is to be revealed;
- the importance of producing the records in the administration of justice, with particular consideration to:
  - the importance of the case;
  - the need or desirability of producing the records to ensure that the case can be adequately and fairly represented; and
  - the ability to ensure that only the particular facts relating to the case are revealed; and
- any allegation of improper conduct by the executive branch towards a citizen.

In Alberta, section 11 of the *Proceedings Against the Crown Act* and section 34 of the *Alberta Evidence Act* govern the procedure for raising Crown privilege.

**Case-by-case privilege applied to private records.** Private records are a third party’s records in which there is a reasonable expectation of privacy. Examples of private records may include medical or therapeutic records, private diaries and social worker activity logs. It does not matter who has possession of the information, but rather whose information it is (*IPC Order 96-020*).

A set of four criteria, called Wigmore’s test, is used to determine, on a case-by-case basis, whether the public interest favours disclosure or non-disclosure of private records. In order to establish that a case-by-case privilege applies to a private record, a public body must provide evidence that the private record meets the following four criteria:

- the communications originated in a confidence that they would not be disclosed;

- this element of confidentiality is essential to the full and satisfactory maintenance of the relationship between the parties;
- the relationship must be one which, in the opinion of the community, ought to be diligently fostered; and
- the injury that would result to the relationship from the disclosure of the communications would be greater than the benefit gained by granting an applicant's request for access to the information under the *FOIP Act*.

In *IPC Order F2008-012*, case-by-case privilege did not apply to communications between a physician and the hospital's chief of staff about a colleague's ability to perform his job. The communications did not originate in confidence, and maintaining confidence would undermine the open and transparent complaint resolution process that had been established for disputes between medical staff. Also, the relationship between a confidential complainant and the chief of staff was not one that should be diligently fostered.

**Settlement negotiation privilege.** This privilege applies to the discussions leading up to a resolution of a dispute in the face of litigation. It promotes the settlement of lawsuits. To apply settlement negotiation privilege, a public body must show that

- litigation exists or is contemplated;
- the communication was made with the express or implied intention that it would not be disclosed to the court in the event negotiations failed; and
- the purpose of the communication is to attempt to effect a settlement (see *IPC Order F2005-030*).

The privilege does not extend to the settlement agreement itself (*IPC Orders F2005-030* and *F2007-025*).

**Statutory privilege.** This is a legal privilege established by an act or by a regulation. Information that is subject to statutory privilege may be withheld under **section 27(1)(a)**.

#### **Information relating to the provision of legal services**

**Section 27(1)(b)** **Section 27(1)(b)** is broader in scope than **section 27(1)(a)** (see *IPC Order F2003-017*). **Section 27(1)(b)** gives a public body the discretion to withhold information that is prepared by or for the Minister of Justice and Attorney General, his or her agent or lawyer, or an agent or lawyer of a public body in relation to a matter involving the provision of legal services.

The Commissioner has said that, in order for the exception to apply, the information in the records must contain "information prepared" – as those words are commonly understood – by or for an agent or lawyer of the Minister of Justice and Attorney General or of a public body, and the records must indicate that the information was prepared by or for such a person (see *IPC Order 99-027*).

The term *legal services* includes any law-related service performed by a person licensed to practise law (see *IPC Order 96-017*).

For example, in *IPC Order 98-016*, some of the records under review were memoranda written to file by Crown prosecutors assigned to the file. They contained a Crown prosecutor's own comments on the case, noting weaknesses, problems with respect to witnesses, etc. They were prepared by lawyers of the Minister of Justice in relation to the criminal prosecution of the applicant. The Commissioner held that **section 27(1)(b)** applied to those records.

**Information relating to the provision of advice or other services**

**Section 27(1)(c)** In order for **section 27(1)(c)** to apply, two criteria must be met:

- the information must be correspondence between any person and the Minister of Justice and Attorney General, his or her agent or lawyer, or an agent or lawyer of a public body; and
- the information in the correspondence must relate to a matter involving the provision of advice or other services by the Minister of Justice and Attorney General, his or her agent or lawyer, or an agent or lawyer of a public body (*IPC Order 98-016*).

A memorandum or note from one employee of a public body to another summarizing a conversation between that employee and the public body's lawyer may meet the two criteria in **section 27(1)(c)** (see *IPC Order 96-019*).

Letters between Crown prosecutors and the RCMP containing requests or suggestions regarding the file, including advice to the RCMP with respect to what charges ought to be laid, were found by the Commissioner to meet both criteria. The letters were prepared specifically in relation to the prosecution of the applicant, and the prosecution of criminal charges is a service provided by the Crown Prosecutors' Office (see *IPC Order 98-016*).

**Privileged information of a third party**

**Section 27(2)** A public body must refuse to disclose information that is subject to a legal privilege where that information relates to a person other than the public body. For **section 27(2)** to apply, there must first be a finding that the information in question is covered by **section 27(1)(a)** (see *IPC Order 96-021*). If **section 27(1)(a)** applies, and the information relates to a person other than the public body, **section 27(2)** prohibits a public body from disclosing that information.

Records in which a public body has discussed or otherwise reproduced a third party's privileged information may also be covered by this exception (see *IPC Order 97-009*).

Even if a record of this nature was disclosed before the coming into force of the Act, a public body must now apply **section 27(2)** and withhold the record if the record is within the scope of the exception (see *IPC Order 97-009*).

If the criteria in **section 27(1)(a)** are not met, there is no privilege, and **section 27(2)** cannot apply (see *IPC Order 99-027*).

If information subject to **section 27(1)(a)** (e.g. privileged information relating to a public body) and to **section 27(2)** (e.g. privileged information relating to an employee



of the public body (third party)) is intertwined, **section 27(2)** (the mandatory exception for privileged information related to a third party) applies to all of the information (*IPC Order F2002-007*).

### Waiver of privilege

If a legal privilege applies to a record, only the party entitled to the privilege may waive it. In order for a waiver to be effective, the party entitled to the privilege must have voluntarily relinquished the right to require that the document remain confidential.

Waiver of privilege depends on intention (*IPC Order 97-009*). Waiver is established when the party entitled to the privilege

- knows of the existence of the privilege, and
- demonstrates a clear intention to forego the privilege.

(*Adjudication Order No. 3*.)

The party claiming waiver of privilege has the burden of proof (*Adjudication Order No. 3*).

There are several indicators that, if present, suggest that a legal privilege has been waived. They include the following:

- an express declaration that the privilege is waived;
- the party entitled to the privilege does not restrict the use of the privileged record by the person to whom it is sent;
- part of a record containing solicitor–client privilege is released or privilege is not claimed for the entire communication on a page (for deemed waiver in such a case, see *IPC Order 96-017*); or
- the record is copied to a third party (as a “cc”) (except where common interest privilege exists – see *IPC Order 97-009*).

It is possible to waive a privilege for a limited purpose. For example, a person may deliver a privileged document to a third party with the intention that no one other than that third party views the document. In that situation the person may be found to have waived the privilege with respect to that third party but not with respect to any other third party.

Privilege is not waived when an individual is obliged to comply with a public body’s requirements under penalty of enforcement proceedings for non-compliance (see *IPC Order 98-017*).

Providing copies of privileged records to other employees within a public body will not waive privilege (see *IPC Order F2003-017*).

Failure by the party entitled to privilege to respond to a third party notice given under the *FOIP Act* does not constitute a waiver of privilege (*Adjudication Order No. 3*).

A public body's disclosure of records in the public interest (**section 32**) does not mean that the public body has waived privilege for all associated records (*Adjudication Order No. 3*).

#### **Exercise of discretion under section 27**

**Section 27(1)** is a discretionary exception. Even if it applies to a record, a public body may choose to disclose it. **Section 27(2)** is a mandatory exception. If it applies to a record or information, a public body must not disclose that record or information.

#### **Severing of information from privileged records**

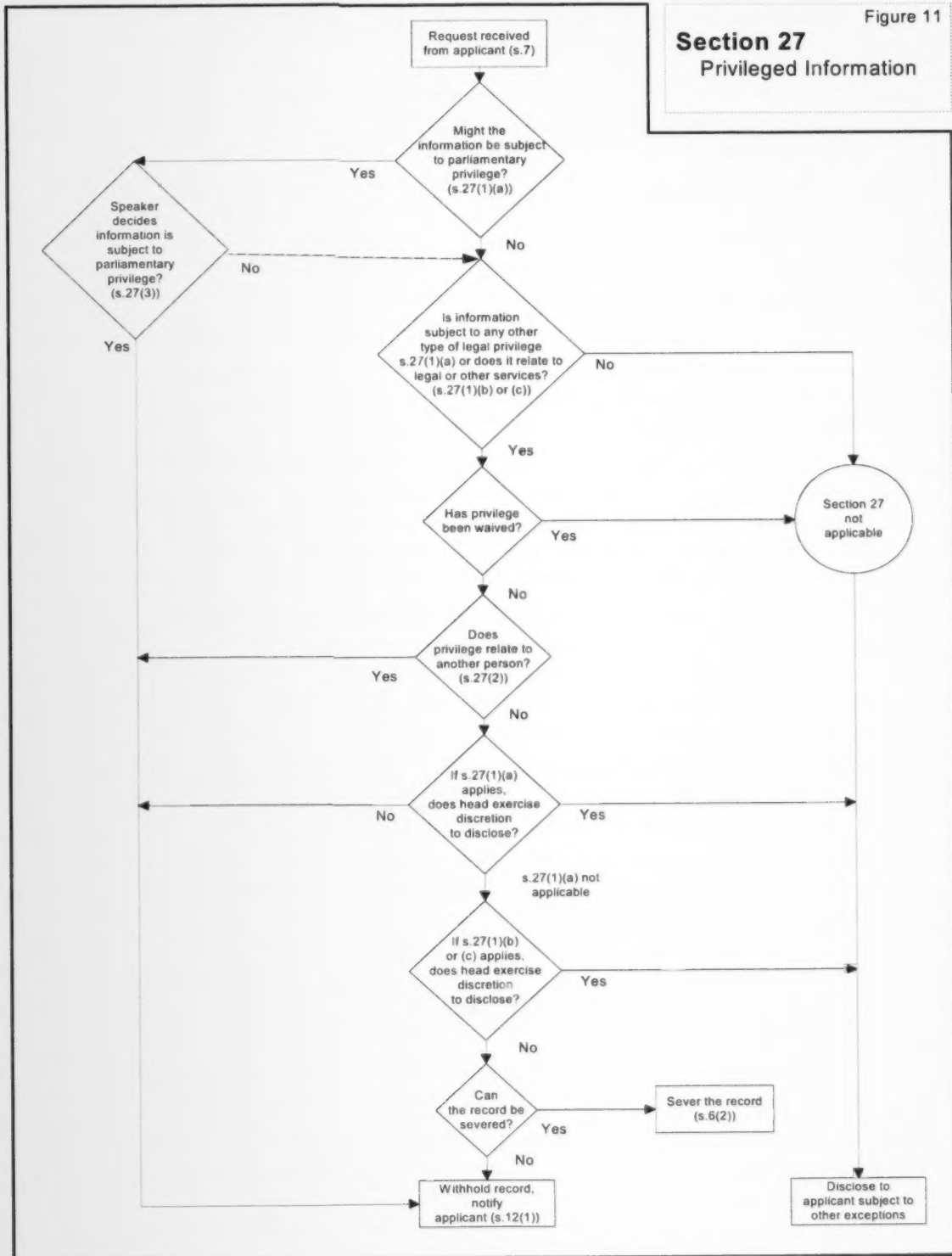
**Section 6(2)** of the Act allows an applicant to request access to part of a record if that information can reasonably be severed from the record. However, **section 6(2)** does not apply to allow severing of documents for which a legal privilege in **section 27(1)(a)** is claimed (see *IPC Order 96-017*). If a legal privilege is claimed for a record, the privilege normally must be applied to the entire record and none of the information in that document may be disclosed.

#### **Applying the exception**

Figure 11 contains a flowchart setting out the steps for applying **section 27**.

Figure 11

## Section 27 Privileged Information



**4.14**  
**Disclosure**  
**Harmful to**  
**Historic**  
**Resources or**  
**Vulnerable**  
**Forms of Life**

**Section 28** provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to result in damage to or interfere with the conservation of

- any historic resource as defined in section 1(f) of the *Historical Resources Act*; or
- any rare, endangered, threatened or vulnerable form of life.

**Section 28** is a discretionary exception.

For the exception to apply, there must be objective grounds to believe that disclosure is likely to result in damage to historic resources or interference with conservation measures.

*Damage* refers to destruction, disturbance, alteration, deterioration or reduction in the value of an historic resource.

**Historic resources**

**Section 28(a)** The provision enables a public body to withhold information about historic resources, which, if disclosed, could result in damage to these resources or interference with conservation measures. If a public body has records that might fall within this exception, it may consult with the ministry responsible for the *Historical Resources Act* (Alberta Culture and Community Spirit) in making a decision on disclosure.

The *Historical Resources Act* defines *historic resources* as any work of nature or of humans that is primarily of value for its palaeontological, archaeological, prehistoric, historic, cultural, natural, scientific or aesthetic interest, including, but not limited to, a palaeontological, archaeological, prehistoric, historic, or natural site, structure or object.

Examples include designated municipal historic resources, designated registered historic resources in private ownership, museum collections, and archaeological and palaeontological sites revealed during a historic resources impact assessment.

**Rare, endangered, threatened or vulnerable forms of life**

**Section 28(b)** In **section 28(b)**, the following general definitions apply.

A *rare form of life* is any species of flora or fauna that is in a special category because it does not occur in great abundance in nature, either because it is not prolific or its population or range has been adversely affected by modern civilization.

An *endangered form of life* is any species of flora or fauna that is threatened with extinction throughout all or a significant portion of its natural range.

A *threatened form of life* is any species of flora or fauna that is likely to become endangered in Canada or Alberta if the factors affecting its vulnerability are not reversed.

A *vulnerable form of life* is any species of flora or fauna that is of concern because it is naturally scarce or likely to become threatened as a result of disclosure of specific information about it.

## 4.15

**Information that is or will be Available to the Public**

**Section 29** provides that a public body may refuse to disclose information

- that is readily available to the public;
- that is available for purchase by the public; or
- that is to be published or released to the public within 60 days after the applicant's request is received.

**Section 29** is a discretionary exception.

**Readily available to the public**

*Section 29(1)(a)* This provision enables a public body to refuse to disclose information that is readily available to the public.

*Readily available to the public* means currently accessible to the general public. For example, the information may be available through a website, in a public library, in a public directory or in a manual available to the public for copying (see *IPC Order F2002-023*). Access may involve a modest cost, such as copying charges.

If an applicant requests information to which this exception applies, the public body must tell the applicant how the information may be accessed. Examples of information that may be readily available to the public include annual reports of public bodies; information about the membership of governing bodies of public bodies; and statutes, regulations and bylaws.

**Available for purchase by the public**

*Section 29(1)(a.1)* This provision enables a public body to refuse to disclose information that is currently available for purchase by the public. This exception allows the public body to follow its normal procedures for selling information, if the public body has a policy of doing so, or to make a decision to publish particular information. The Act is not intended to replace existing procedures for access to information (**section 3(a)**).

*Available for purchase by the public* means that a publication is generally available for purchase from the public body or a government or other bookstore. The information must be available to the general public, not only to a limited group such as realtors or an interest group (see *IPC Order 98-004*).

If an applicant requests information to which this exception applies, the public body must tell the applicant where the publication may be purchased. Examples of information available for public purchase include maps, research reports, catalogues, manuals and electronic or print subscription services.

Where records are annotated by a public body, they become new records. If the new records are not publicly available, then **section 29(1)(a)** will not apply (see *IPC Order 2001-009*).

**To be published or released within 60 days**

*Section 29(1)(b)* This provision allows a public body to decide whether or not to withhold information that will be published or released within 60 days of the applicant's request.



*Published* means made available for public sale or made available at no cost, to the public through print or electronic media, including posting on a website.

*Released to the public* means made available to the public at large either through active dissemination channels or through provision of the information at specific locations (e.g. public libraries).

Situations arise when a request is made for information that is about to be published. There may be a number of reasons to withhold the information under **section 29(1)(b)**. For example, where a publication is required to be tabled in the Legislature, it may be appropriate for the Minister or head to exercise his or her discretion not to release the information first through the *FOIP Act*. It may also be reasonable to not disclose the information through the *FOIP Act* if the information is scheduled to be released in conjunction with a public event or public announcement or is to be published within 60 days of the applicant's request.

The exception covers only the manuscript being published and not related data or research and background material. These records have to be dealt with separately, if requested, or if the applicant does not believe that the request is satisfied by receipt of the publication.

**Section 29(1)(b)** may only be applied if there are no legal impediments to publishing, such as **Part 2** of the *FOIP Act*.

The 60 days for publication or release is from the date of receipt of the applicant's request and not from the date when a response is made to the request. It is important that a public body ensure that the requested records will be published or released to the public within the 60-day time frame established by the provision.

A public body does not have to consult with, or provide notice to, third parties with respect to information that is available to the public or will be published or released within 60 days of the applicant's request (**section 30(1.1)**). It is presumed in these cases that the public body has already considered any confidentiality or privacy matters related to the information before deciding to make it publicly available.

### **Notification of applicant**

**Section 29(2)** **Section 29(2)** requires the public body to notify an applicant of the publication or release of information that the head has refused to disclose under **section 29(1)(b)**.

Such notification should provide

- the date of publication or release;
- the specific location where the applicant can have access;
- how access will be given;
- the purchase price, if applicable; and
- any other information that the public body is required to give the applicant under **section 12(1)** of the Act.

If there is no charge for the publication, the public body could simply provide a copy to the applicant on publication.

**If information is not published or released**

*Section 29(3)* If the information is not published or released within 60 days after the applicant's request is received, the public body must reconsider the request. This must be done as if it were a new request received on the last day of that period, and access to the information must not be refused under **section 29(1)(b)**.

This means that on the 60th day the public body is required to consider the applicant's request as a new request with 30 days to respond, dating from that day. The public body cannot employ the **section 29** exception in any consideration of the new request.









## 5.

# THIRD PARTY NOTICE

### Overview

This chapter covers

- who is a third party;
- when third party notice is required;
- the notice process for third parties and applicants;
- the response from a third party;
- the decision by a public body, and
- time limits.

See FOIP Bulletin No. 10: *Third Party Notice*, published by Access and Privacy, Service Alberta, for more detailed information on this topic.

Many public bodies hold large quantities of information about individuals, companies, non-profit groups and other third parties. The *FOIP Act* includes a consultation process for situations where disclosure of this information might result in harm to a third party or be an unreasonable invasion of a third party's personal privacy (see sections 4.2 and 4.3 in Chapter 4). The Act provides for notification of third parties when access to records containing such third party information is requested.

*Third party* is defined in **section 1(r)** as a person, a group of persons, or an organization other than an applicant or a public body. Third parties include individuals, sole proprietorships, partnerships, corporations, unincorporated associations and organizations, non-profit groups, trade unions, syndicates and trusts (see *IPC Order 98-008* for examples of third parties that required notification). An employee of a public body can also be a third party (*IPC Order 96-019*).

A person authorized to exercise the rights of an individual under **section 84** of the *FOIP Act* is *not* a third party.

### 5.1 When to Give Third Party Notice

#### Notice *must* be given under section 30

A public body *must* give notice to a third party under **section 30(1)(a)** if

- the public body is considering giving access to records, and
- the exception for third party business information (**section 16**) may apply to information in the records.

Similarly, a public body *must* give notice to a third party under **section 30(1)(b)** if

- the public body is considering giving access to records, and
- the exception for personal privacy (**section 17**) may apply to information in the records.

For example,

- a public body that is considering giving access to third party commercial information that was supplied in confidence must give notice to the third party if there is any question as to whether the disclosure could reasonably be expected to cause significant harm to the third party's competitive position or any of the other outcomes listed in **section 16(1)(c)**;
- a public body that is considering giving access to third party personal information must give notice to the third party if there is any question as to whether the disclosure may be an unreasonable invasion of the third party's personal privacy under **section 17**.

If a public body is responding to a continuing request (**section 9**), notice under **section 30(1)** must be given each time the public body is considering giving access to records that may be subject to the exception for business information in **section 16** or the exception for personal privacy in **section 17**. A one-time third party consent would not be sufficient for the purposes of **section 30** because a third party cannot consent to the disclosure of records that have not yet been created.

If a public body has made a decision regarding disclosure of third party information in response to a request, and there is a new request for the same information, the public body may be required to give notice again – and may arrive at a different decision after taking into consideration a change in circumstances (see *IPC Order F2004-013*).



There is no obligation to give third party notice when a public body is *not* intending to give access to third party information (*IPC Order 99-007*).

### **Notice *may* be given under section 30**

The Act expressly states that a public body *may* (but is not required to) give notice to a third party if

- the public body has determined that **section 16** or **section 17** applies to the third party's information in a record, and
- the public body does not intend to give access to the information.

A public body may decide to give notice when it is not required to do so to allow a third party to provide reasons for not disclosing the information. For example, if a public body has decided that disclosure of third party business information could reasonably be expected to cause significant harm to the third party's competitive position, the third party may be able to provide information to support the public body's non-disclosure decision.

A public body may also decide to give notice when it is not required to do so to allow a third party to consent to the disclosure. For example, a media applicant may have made a request to a post-secondary educational body for personal information relating to the educational history of a public figure. Disclosure of this type of information is presumed to be an unreasonable invasion of a third party's personal

privacy (under **section 17(4)(d)**). However, the public body may choose to provide an opportunity for the public figure to consent to disclosure of the information.

The Information and Privacy Commissioner has said that he cannot impose a duty upon a public body to give notice where the Act does not establish a duty to do so (*IPC Order 97-018*). This is the case even if there is some likelihood that the third party would give consent if notified.

However, if the applicant requests a review, the Commissioner may, under **section 67(1)(a)(ii)** of the Act, give a copy of the request for review to any person, including a third party who, in the Commissioner's opinion, is affected by the request for review.

If notice is given under **section 30** and the third party consents to disclosure of the third party information, the record cannot be withheld under **section 16** or **section 17**, as the case may be. The public body cannot refuse to disclose the information unless another exception applies to it.

### Notice requirement in section 30 does not apply

The Act specifically states that there are two instances where the notice requirement in **section 30(1)** does not apply.

The first is where the head of the public body has decided to withhold information under the exception for information that is or will be available to the public (**section 29**). For example, if a public body has decided to issue a news release containing third party business or personal information on a date in the near future, the Act allows the public body to refuse to disclose the information in response to an access request. **Section 30(1)** does not apply in these circumstances; and the public body does not need to notify the third party.

The second instance where the notice requirement in **section 30(1)** does not apply is where a public body has decided to disclose a record containing information described in **section 17(2)(j)** (enrolment in an educational program, attendance at a public event related to a public body, receipt of an honour or award granted by a public body). Disclosure of this information is not an unreasonable invasion of personal privacy unless the third party has requested that the information not be disclosed under **section 17(3)**. **Section 30(2)** states that the requirement to give notice established in **section 30(1)** does not apply to a record containing information to which **section 17(2)(j)** applies.



Public bodies should take steps to give individuals an opportunity to request non-disclosure under **section 17(3)** when personal information subject to **section 17(2)(j)** is collected, because third party notice will not be given in these cases.

In addition, the notice requirement in **section 30(1)** does not apply if the public body has decided to give access to third party information on the basis that the information is clearly not subject to **section 16** or **section 17**. The clearest example of this would be where the third party has already given unqualified consent to disclosure of

requested business information and has advised the public body that it does not wish to receive notice of future requests for the same information.

### **Section 30 not relevant**

There are a number of cases where a third party's interests may be affected, but a public body does not need to consider **section 30**.

The notice requirement is not relevant to a request for records that may be subject to an exception in the Act other than **section 16** or **section 17**. This is the case even if another mandatory exception (e.g. the exception for legal privilege of a third party in **section 27(2)**) applies to information in the records.

The same is true for records that may be subject to discretionary exceptions. **Section 30** is not relevant to a request for records that are subject to the exception for advice from officials (**section 24**), for example.

**Section 30** is also not relevant to the disclosure of personal information under **Part 2** of the Act. A public body may disclose personal information under **section 40(1)(b)** – the provision for disclosure that is not an unreasonable invasion of privacy under **section 17** – after the public body has done a complete analysis under **section 17** and determined that the disclosure would not be an unreasonable invasion of a third party's privacy. (If the public body believes that it would be appropriate to give notice to a third party, it may be advisable to ask the person who requested the information to submit an access request under the *FOIP Act*. The third party would then be given notice of the request.)

Notice is not given under **section 30** to a public body, since a public body is not a third party as defined in the *FOIP Act* (**section 1(r)**). Nor is notice given under **section 30** for the purpose of consulting with a government body in another jurisdiction.

Any notice that is given to a third party or other person in circumstances where **section 30** has no application has no standing under the Act. The third party or other person would have no right to request a review by the Commissioner of the public body's decision on disclosure of the information in question.



A public body that gives notice to a third party, formally or informally, must not disclose the identity of an individual applicant.

## **5.2 Initiating the Third Party Notice Process**

### **Notice where practicable and as soon as practicable**

**Section 30(1)** requires that any third party notice be given “where practicable and as soon as practicable.”

Giving notice “where practicable” means giving notice (when it has been decided that notice must or may be given) unless it has not been possible to locate and notify the third party after making reasonable attempts to do so. Public bodies are expected to

use only their own records and publicly available resources to locate an address for a third party.

Conducting a search through a corporate registry may provide information on the status of a company, organizational and name changes, and the most current contact information.

A public body should not rely on particulars about a third party, such as name, address or phone number, that are contained in historical records, since the information may no longer be accurate.

If there is any doubt as to the third party's contact information, the public body may need to adapt its notification process to ensure there is no breach of privacy or confidentiality in the course of the notification process. In *IPC Order 2000-019*, it was decided that the impracticability of giving notice to a third party was a relevant circumstance that weighed in favour of not disclosing the third party personal information.

Giving notice "as soon as practicable" means giving notice as soon as reasonably possible after determining that a third party needs to be consulted. This enables the public body to respond to the request in a timely manner.

**Section 30(5)** of the *FOIP Act* says that when notice is provided to the third party, notice must also be provided to the applicant. Where possible, these notices should be given at the same time.

Separate notice must be given to each third party whose interests may be affected by disclosure of the information. Where a public body is notifying multiple third parties, and especially where the public body is notifying multiple third parties about the same or related records, the public body should issue the third party notices on the same day.

### 5.3

#### Time Limits

#### Time limits under sections 30 and 31

Time limits for responding to access requests are set out in **section 11(1)** and **section 14** of the Act. When a public body is processing a request involving third party notice, the Act requires the public body to delay responding to the request so as to allow the third party time to exercise their rights under the Act, including their right to request a review by the Information and Privacy Commissioner. The time limits for the parties to exercise their rights are set out in **sections 30** and **31**.

*Prior to giving notice* to a third party, a public body may extend a time limit under **section 14(1)(a), (b) or (c)** or **section 14(2)**. The permission of the Commissioner may be required in certain circumstances. Extensions under **section 14(1)** and **(2)** are discussed in Chapter 3, section 3.3.

*After giving notice* under **section 30**, a public body must observe the time limits set out in **section 31**. Extension of the time limit for responding to the request in order to comply with **section 31** is permitted under **section 14(3)**. The permission of the Commissioner is not required.



The applicable time limits are as follows:

- a third party has 20 days to respond to the notice (**section 30(4)(c)**);
- no decision can be made until the third party's response is received, or 21 days after notice is given, whichever comes first (**section 31(1)**);
- the public body must make a decision whether to grant access or not and notify the third party and applicant of this decision within 30 days after third party notice is given (i.e. the public body has at least 10 days to consider the response from a third party and make the decision) (**section 31(1)**);
- after the public body's notice of a decision is given, a third party has 20 days to ask for a review (**section 31(3)**); and
- after the public body's notice of a decision is given, the applicant has 60 days to ask for a review (**sections 31(4) and 66(2)**).

The Act does not allow a public body to extend any of the time limits in **section 31** for any reason.

#### **Effect of time limits**

The 20-day time period allowed for a third party to respond to a notice begins on the day after the third party notice is given (i.e. the day after the public body sends the notice), not the date the third party receives it. The date on which the notice is sent is the date marked on it indicating posting or electronic transmission (e.g. the postmark for regular mail, and the transmission date for e-mail or facsimile). For example, if a public body sends a third party notice by regular mail and the envelope is postmarked March 1, the third party has until the close of business on March 21 to respond. For this reason, public bodies should choose a delivery method that ensures that notice is given promptly.

Contacting a third party prior to giving written notice is a good practice. It enables the public body to explain the process, the importance of responding, the consequences of not responding and the time lines. See FOIP Bulletin No. 10: *Third Party Notice*, published by Access and Privacy, Service Alberta, for other practical considerations.

#### **Time limit extensions for complex requests**

If a public body is processing a request that requires an extension for several reasons – for example, the request involves a large number of records, will necessitate consultation with another public body, and will also require third party notice – the public body should extend the time limit for responding under **section 14(1)** first. Once notice has been given under **section 30**, the public body can rely only on **section 14(3)**. **Section 14(3)** allows a public body to extend the time limit for responding to a request to enable the public body to comply with the requirements of **section 31**.

If the request involves multiple third parties, the most practical method of working with the time limits is to ensure that all third parties have been identified before beginning the notification process, then to send out all the notices at the same time.

From time to time, a public body identifies an additional third party late in the processing of the request. This may happen because additional records are identified after the initial search or because a third party notice results in information that suggests further that the public body should provide notice to another third party. In these cases, it is recommended that the public body make its decision concerning access to the records on which it has given notice and provide a response to the request with respect to those records. The public body should delay its response only with respect to the records for which the notification process is not complete. Although the Act does not specifically provide for responding to a request in part, this approach to timely release of records is consistent with the spirit of the Act.

Under these circumstances, if the applicant were to request a review, the time limit for requesting the review would be 60 days from the day on which the *final* response to the request was given.

The applicant has the right to make a complaint to the Information and Privacy Commissioner about any time limit extension.

### **Manner of giving notice**

**Section 83** requires that any notice or other document to be given to a person under the Act be given

- by sending it to that person by prepaid mail to the last known address of that person;
- by personal service;
- by substitutional service if so authorized by the Commissioner;
- by facsimile telecommunication; or
- in electronic form other than facsimile telecommunication if the person to whom the notice or document is to be given has consented to accept the notice or document in that form.

Public bodies should choose a delivery method that is expeditious and convenient for the third party, but which is also efficient and cost-effective for the public body. Regular mail is not recommended. If there is a small volume of records, the records can be faxed to the third party. For larger volumes, records should be sent by courier or priority post. Prompt delivery will allow the third party as much time as possible to respond.

If sending the notice by fax or other electronic means, care should be taken to prevent unauthorized disclosure of third party information. It may be necessary to telephone the third party before sending the notice to identify the individual best qualified to deal with it or to advise of the electronic transmission. For some measures recommended by the Commissioner, see *Guidelines on Facsimile Transmission* (revised 2002). Public bodies that are government departments or agencies should also refer to the requirements for transmission of personal information in the *Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile* (revised July 2002), developed by the Office of the Corporate Chief Information Officer.

See Chapter 2, section 2.6 for further discussion on the manner of giving notice.

#### 5.4

#### Notice to a Third Party

#### Content of third party notice

Section 30(4) states that a third party notice must

- state that a request has been made for access to a record that may contain information the disclosure of which would affect the interests or invade the privacy of the third party;
- either include a copy of the record, or the part of it containing the information in question, or include a full description of the contents of the record involved; and
- state that, within 20 days after the notice is given, the third party may, in writing, either consent to the disclosure or make representations to the public body explaining why the information, in whole or in part, should not be disclosed.

If a record that is the subject of a third party notice contains personal information about other third parties, it may be best simply to describe the record in the notice. If a public body sends a third party a record that contains personal information of other third parties, the public body risks the unintentional disclosure of that personal information (see *IPC Order 99-030*).

**Model Letter L** in Appendix 3 sets out the various options for third party notice. The notice provides a summary of the particular exception involved (either **section 16** or **section 17**). It also provides an explanation of the points that a third party should address in any representations as to why information should not be disclosed. The version of this letter relating to **section 16** notes, in particular, the importance of providing clear and specific information relating to any harm that may be expected to result from disclosure of records to which **section 16** may apply.

Although the Commissioner stated in *IPC Order 99-023* that he did not have jurisdiction to review the content of a third party notice, efforts should be made to ensure that the third party understands the significance of the notice.

A public body must decide whether to withhold or grant access to third party information on the basis of factors relevant to the applicability of **section 16** or **section 17**. However, the public body can consider comments or statements from a third party that may be relevant to other exceptions, such as **sections 18, 20, 21, 24, 25** and **27**, when it is considering whether any other exceptions apply to the record. Also, if there is a question as to whether **section 27(2)** may apply, the third party that has privileged information should be consulted. Consultation on exceptions other than **sections 16** and **17** is not notice for the purposes of **section 30** and has no standing under the *FOIP Act*.



**Third party notice must be in writing. A verbal notice is not satisfactory for the purposes of section 30. The identity of an applicant must not be included in the notice sent to the third party, unless the applicant has consented to this disclosure (see *IPC Investigation Report 98-IR-009*). The notice must include the name, job title and telephone number of the person within the public body that the third party may contact for more information.**

Good communication with the third party ensures a smooth notification process and promotes better understanding of the third party's representations when determining the applicability of the exception.

The identity of a third party business should be confirmed before sending a third party notice. However, if the identity of the most appropriate person to receive the notice is unclear, the public body may wish to add a comment to the notice stating that the public body should be notified if the recipient is not the appropriate person to receive the notice, or if the recipient is aware of another third party that may also have an interest in the information.

#### 5.5 Notice to Applicant

**Section 30(5)** provides that, when notice is given to a third party, the public body must also provide a notice to the applicant.

The notice must state that

- the requested record(s) may contain information the disclosure of which would affect the business interests or invade the personal privacy of a third party;
- the third party is being given an opportunity to make representations respecting disclosure; and
- a decision whether or not to give access to the requested record(s) will be made within 30 days after the date of notice to the third party.

A model notice to an applicant is included as **Model Letter M** in Appendix 3.

#### 5.6 Response from Third Party

In deciding whether or not to give access to all or a portion of the requested record(s), the public body must consider any third party responses received in reply to notices given under **section 30** which are pertinent to **section 16** or **17**, as applicable. The response from the third party must be in writing.

**Section 31(1)** provides that a public body must decide whether or not to give access within 30 days of giving notice. A decision cannot be made until the third party responds, or on the 21st day after notice is sent, whichever comes first.

### **Consent**

If the third party consents in writing to disclosure of the information, the public body must release the information unless another exception in the Act applies to it.

Where the third party is an organization, the public body should be reasonably satisfied that the person giving consent to disclose the information on behalf of an organization is an officer, employee or corporate officer authorized to provide such consent.

### **Representations opposing disclosure**

If a third party makes representations as to why the information should not be disclosed, the public body must consider the representations in reaching a decision on access.

If there is any doubt that the third party has understood the significance of the notice or the criteria that apply in decisions regarding access, the public body should contact the third party by telephone to discuss the matter.

### **Non-response**

If a third party does not respond to the notice by the 21st day after the notice was given, the public body must make a decision based on the information available.



Failure to respond to a notice does not imply that the third party has consented to the disclosure of the information.

A public body should contact the third party by telephone, fax or e-mail to discuss why a response has not been made and advise the third party of the consequences of not responding. The opportunity for contact extends up to the point of disclosure of the information. It may be helpful, in the event of a review by the Information and Privacy Commissioner, for the public body to be able to provide documentation of its efforts to contact a third party.



If the third party requests a few extra days to respond and the public body agrees, these days would be subtracted from the 10 days in which the public body must make a decision. The Act does not allow the public body to extend its time to make a decision in order to give a third party more than 20 days to respond. After notification of the public body's decision, the third party still has 20 days to request a review by the Commissioner of the public body's decision to disclose the third party's information.



## 5.7 Decision by Public Body and Notice of Decision

The public body is required to decide whether or not to give access to all or part of the record within 30 days after third party notice is given.

**Section 31(1)** states that the public body must not make this decision until after the third party has had an opportunity to respond to the notice. Since the third party has up to 20 days to respond, the public body cannot make a decision on access until the earlier of

- 21 days after the notice was given; and
- the day a response is received from the third party.

**Section 31(2)** provides that once a public body makes a decision on access, it must give written notice of this decision, including reasons for the decision, to both the applicant and the third party. The content of the notice will vary according to circumstances.

### **When a public body decides to grant access to the record**

#### ***Notice to applicant***

The public body must inform the applicant of the decision and the reasons for it. The public body must also provide notice that access will be provided 21 days after the date the notice of the decision is given if the third party does not ask for a review by the Information and Privacy Commissioner.

#### ***Notice to third party***

Whether or not the third party responded to the notice, the public body must inform the third party of the decision and the reasons for it, and provide notice that the third party can request a review by the Commissioner of the public body's decision within 20 days. This 20-day period is calculated from the day after the public body gives the notice, not from the date the third party receives it. The relatively short period for the third party to request a review is based on two considerations. First, the public body must exercise its decision-making authority properly, regardless of whether the third party responds to the notice or not. Second, the third party will already have had at least 20 days after notice was given to make representations as to why disclosure should not be given. Therefore, the third party should not require much additional time to decide whether or not to request a review.

The public body should set out its reasons for the decision in a comprehensive way. There are two benefits of this: first, the reasons will assist the third party in understanding how the Act applies to the information; second, the public body's decision may be the subject of a request for review by the Commissioner (*IPC Order 98-006*).

If the third party does not request a review within the 20-day period, the applicant is given access to the records that were the subject of third party representations on the 21st day. A public body must contact the Office of the Information and Privacy Commissioner to determine whether a request for review has been submitted. The applicant is not given access to any record or part of a record that is the subject of the review until the review is completed.

If the review affects only some of the records proposed for disclosure, the public body must release the remainder of the records to the applicant unless they are subject to other exceptions. The outcome of the review determines whether or not access is given to any record that is the subject of the review.



The public body cannot disclose the information until after the 20 days allowed for the third party to request a review have passed (see *IPC Order 98-006*).

Even if the third party consents to the disclosure of the records, the public body should not disclose the records before the expiry of the time allowed to request a review. This is because misunderstandings may arise regarding the authority of the employee or officer who consented or what the third party believed it was consenting to disclose.

### **When a public body decides to deny access to the record**

#### ***Notice to applicant***

The public body must inform the applicant of its decision and the reasons for it, and provide notice that the applicant may, within 60 days, request a review of the decision by the Commissioner in accordance with **section 65(1)**.

#### ***Notice to third party***

The public body must inform the third party of its decision and the reasons for it, and that the applicant may, within 60 days, request a review of the decision by the Commissioner.

**Model Letters N and O** in Appendix 3 outline the options for these types of notices.

In *IPC Order 2000-014*, the Commissioner outlined his expectations as to how public bodies should notify applicants and third parties of their decisions. When giving notice of a decision under **section 31**, the public body should avoid using the words “partial access.” The response should specify which records are going to be disclosed and which records cannot be disclosed. The Commissioner’s expectations are discussed in more detail in FOIP Bulletin No. 10: *Third Party Notice*, published by Access and Privacy, Service Alberta.

### **Application of third party notice**

Figure 12 contains a flowchart setting out the process for giving third party notice.

Figure 12

### Sections 16 and 17 Third Party Notice

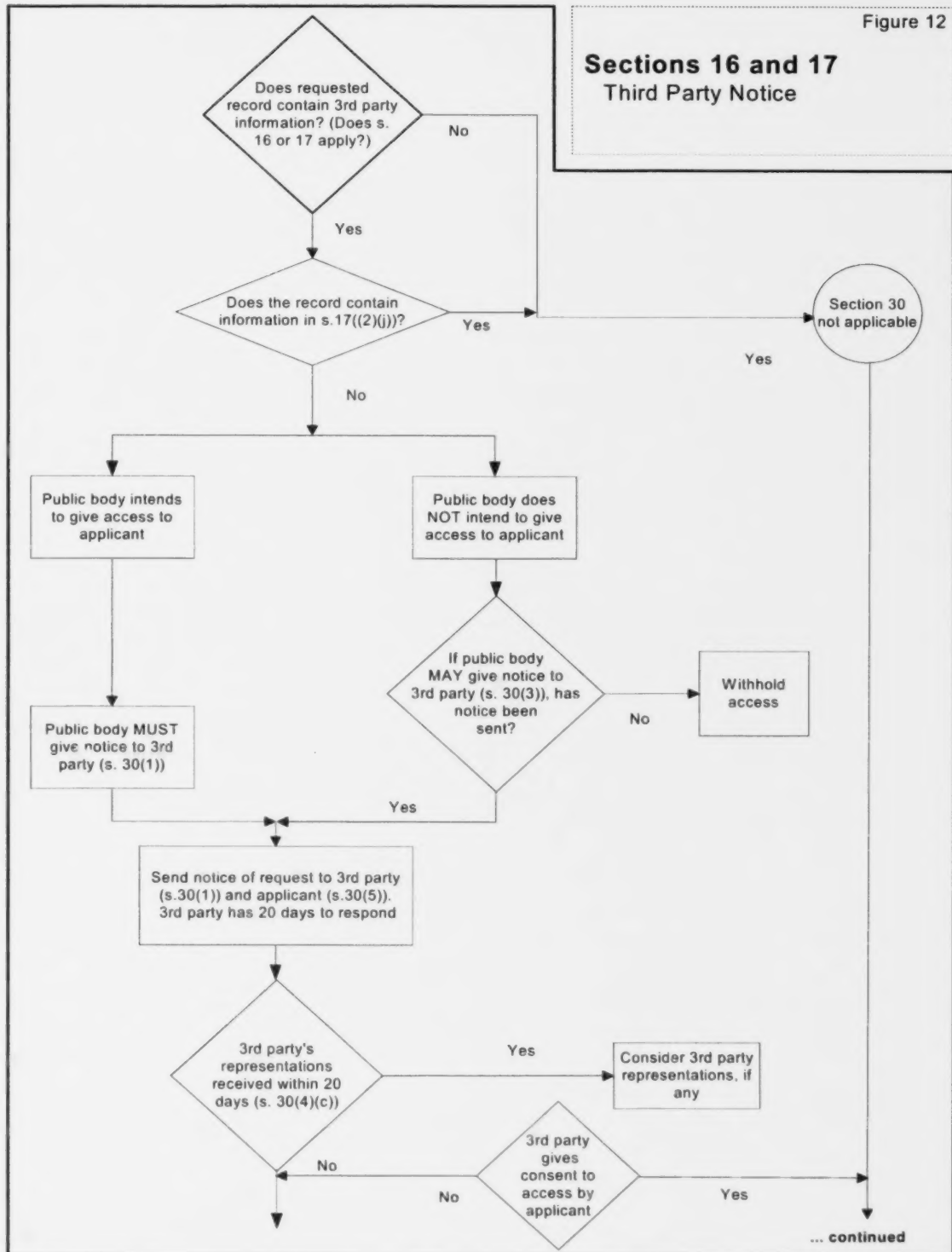
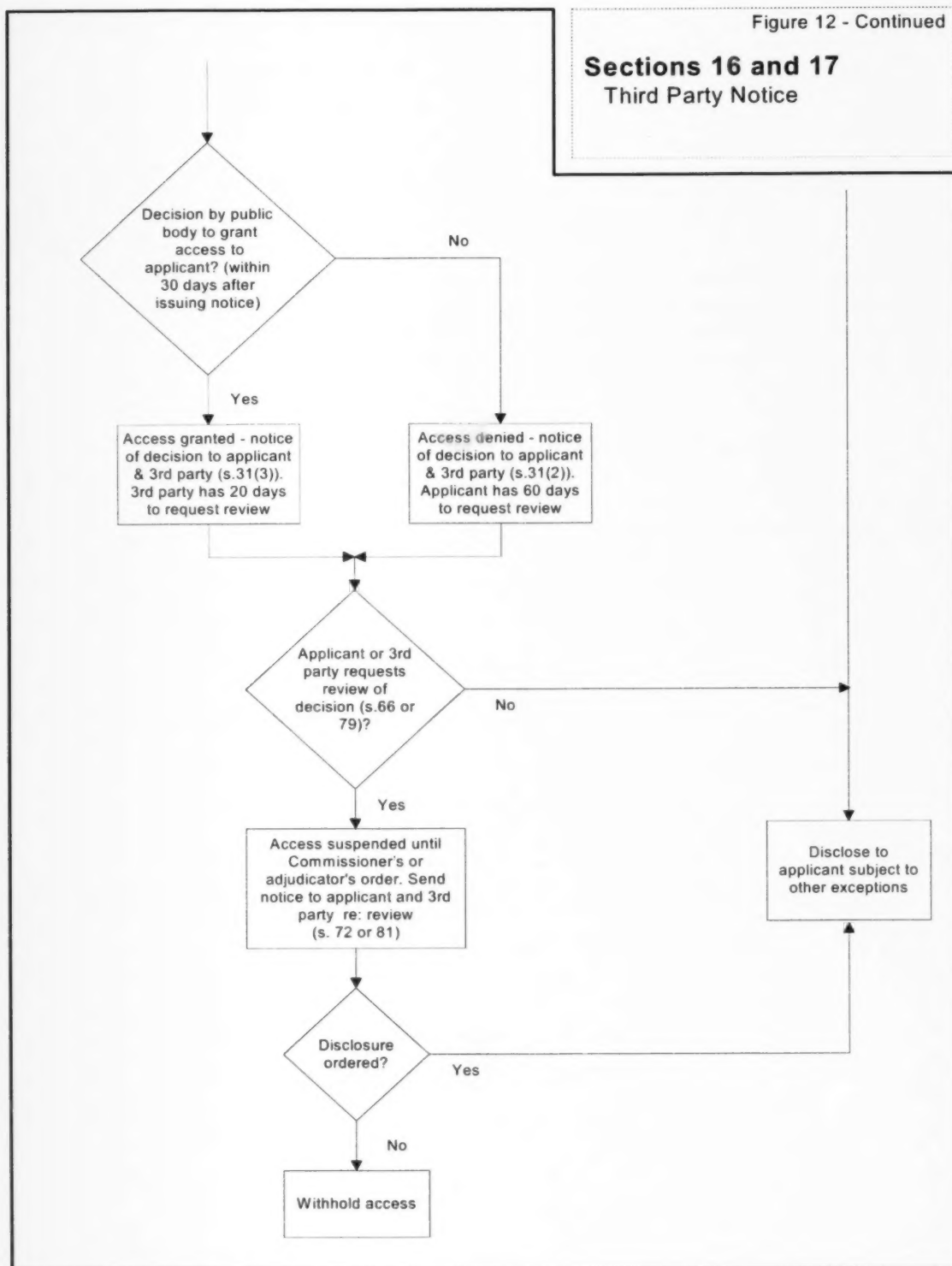


Figure 12 - Continued

**Sections 16 and 17**  
Third Party Notice







## 6.

## DISCLOSURE IN THE PUBLIC INTEREST

## Overview

This chapter covers

- when disclosure in the public interest is required;
- how to determine public interest;
- the scope of **section 32**;
- notice requirements; and
- review of a failure to disclose information.

## 6.1

When  
Disclosure  
is Required**Information to which section 32 applies**

The head of a public body must, without delay, disclose to the public, to an affected group of people, to any person or to the applicant

- information about a risk of significant harm to the environment or to the health or safety of the public, an affected group of people, a person or the applicant (**section 32(1)(a)**); or
- information the disclosure of which is, for any other reason, clearly in the public interest (**section 32(1)(b)**).

**Section 32** overrides all other sections of the Act. Any information that meets the criteria set out in the provision must be disclosed, even if there has not been a formal access request under the Act.

This means that if **section 32(1)(a)** or **(b)** above applies, a public body must disclose information, including personal information if necessary, despite

- **section 17**, which sets out the exception to disclosure of personal information if it would be an unreasonable invasion of a third party's personal privacy; and
- **section 40**, which sets out the purposes for which personal information may be disclosed.

**Section 32(1)** cannot be applied to records that are excluded from the operation of the Act (*IPC Order 2000-034*). For example, **section 32(1)** does not apply to the disclosure of health information by a public body that is a custodian under the *Health Information Act*. Health information, as defined in the *Health Information Act*, that is in the custody or under the control of a custodian, as defined in that Act, is excluded from the application of the *FOIP Act* under **section 4(1)(u)**. Any disclosure of health information by a custodian under the *Health Information Act* is subject to that Act's disclosure provisions.

The public interest disclosure provision represents a very significant exception to the rules for privacy protection because it could involve a considerable invasion of personal privacy. Any decision by the head of the public body to disclose under

**section 32** of the Act should be carefully considered and rationally defensible (see *IPC Investigation Report 98-IR-011*).

### Disclosure without delay

The provision requires that action be taken *without delay*. The assumption is that any situation that warrants consideration of disclosure under **section 32** requires quick action. No delay should occur where disclosure is demanded by events that could have an impact on public safety or where disclosure is in the public interest. The actual assessment of what constitutes without delay must be made on a case-by-case basis. Some factors that should be considered in the assessment are as follows:

- the level of harm anticipated;
- the degree of risk that the harm will occur;
- the imminence of the harm, that is, whether there is a clear and present danger of significant harm;
- measures that could be taken to avoid the harm and the amount of time required for these measures, and whether the release of information would likely reduce the risk of the harm;
- the importance of consulting with other public bodies whose interests may be affected by the disclosure;
- the right of a third party to make representations; and
- the right of the public to make informed choices about the risks to which they are exposed.

---

## 6.2

### Nature of Disclosure

### Records and information

**Section 32** refers to *information*, not *records*. Where a request for disclosure in the public interest is made by an applicant as part of a FOIP request, the decision of the public body will, most likely, be focused on particular records.

Where no FOIP request is made but the public body is considering disclosure in the public interest to the general public, an affected group or a person other than an applicant, the emphasis will almost always be on information as opposed to records. Disclosure might be of the facts surrounding an event or issue, as opposed to the documents recording those facts (see *IPC Order 97-009*).

The fact that **section 32** applies to *information* rather than *records* means that the obligation to release information does not depend on the existence of recorded information (*IPC Order 96-011*).

The reference to *information* in the wording of this section also means that the investigation of a **section 32** decision will not necessarily result in the release of a specified record to an applicant. Ultimately, the head of a public body may release the actual record, a summary of it or a warning of the risk based on the content of the record (*IPC Orders 96-011* and *97-009*). For example, a public body might release the location, nature and extent of the contamination of a building or site but not necessarily all the scientific, exposure, emergency response and property records that relate to the event.

**Section 32** anticipates disclosure in four different ways:

- to the public generally;
- to an affected group of people;
- to any person; or
- to an applicant making a request.

In all cases, only the minimum amount of personal information necessary to alert the public affected about the risk should be disclosed (see *IPC Investigation Report 98-IR-011*).

#### ***Disclosure to the public***

Where the public interest dictates disclosure to the general public, a public body must ensure that the information is released in a manner designed to reach the public at large. This could include the use of radio, television, newspapers, and electronic networks.

For example, disclosure about an armed or dangerous criminal who is suspected to be in a particular area of Alberta would be made to the general public in that particular area.

#### ***Disclosure to an affected group***

Where the information relates to circumstances that affect only a specific group of people, rather than the public at large, the head must ensure that effective ways are used to reach the affected group. If the information is of a sensitive nature, it is important that steps are taken to ensure that only the affected group is informed.

For example, if a safety hazard, such as an unstable trench, were discovered at a workplace, only those people on site who could come into contact with the hazard before it was fixed would need to be warned.

#### ***Disclosure to any person, including an applicant***

Where information relates to any person, including an applicant, the public body must employ notification measures that provide the information to the person concerned and no one else, unless the public interest dictates wider disclosure of the information.

An example would be disclosure of the fact that an individual has been released on parole and continues to threaten the safety of his or her spouse.

### **6.3 Public Interest**

#### **Information to be disclosed**

**Section 32** provides for disclosure in the public interest where the information is

- about a risk of significant harm to the environment or to the health or safety of the public; or
- for any other reason, clearly in the public interest.

***Disclosure of information about a risk of significant harm to the environment or to public health or safety***

**Section 32(1)(a)** This provision applies to information that reveals a risk of significant harm to the general public, a specific group of people, or an individual, including an applicant.

*Risk of harm* means the chance or danger of injury, damage or loss.

The determination that there is a risk of harm to the environment or to public health or safety is usually made by professionals working for the public body or contracted by the public body to assess situations where there is a possible risk of harm. Determining the nature and extent of the risk is part of the management process.

Since this provision refers to *significant* harm, the head of a public body must believe that the risk of harm is considerably greater than in normal circumstances.

*Harm to the environment* refers to the damage to or degradation of any component of the earth, including air, land, and water; any layer of the atmosphere; and any organic and inorganic matter. Harm to the environment also includes damage to, or degradation of, the interacting natural systems that include components of these things, through either natural calamity or illegal or improper use. An example of a risk of significant harm to the environment might be information about toxic emissions from an industrial plant.

*Harm to health* means damage to the well-being of the body or mind of an individual, or the health of the general public. An example of a risk of significant harm to health might be the presence of contaminants or a highly contagious virus in school buildings or contamination of a water supply.

*Harm to safety* means injury to the individual or to the collective condition of being free from danger or risk. A risk of significant harm to safety might be created by a natural gas leak or a bomb threat in a populated area.

**Section 32** of the Act, together with the Alberta Justice Protocol for the application of the provision, has been used, for example, by law enforcement bodies to disclose personal information about the location of a violent offender released from a correctional facility in cases where the individual is still considered to be a serious risk to a community (see *IPC Investigation Report 98-IR-011*).

In another example, where an applicant requested a Contamination Assessment Report on the site of a former service station but the report did not show an immediate or significant risk to the environment or to public health or safety, the public body was not required to disclose the report under **section 32(1)** (see *IPC Order 98-017*).

***Disclosure of information clearly in the public interest***

**Section 32(1)(b)** This general provision is intended to cover any other situation where the head of a public body may decide that disclosure of information is in the public interest.



### Determination of public interest

Disclosure of the information must be *clearly in the public interest*. This determination must be made on a case-by-case basis. Public bodies must balance the public interest in releasing the information with the public and private interests in protecting the information.

Public bodies should refer to *IPC Order 97-018* (which summarizes *Adjudicator's Order 96-014* and *IPC Order 96-011*) as well as *IPC Order 98-019*. The Information and Privacy Commissioner noted that the Legislature did not intend **section 32** to operate simply because a member of the public asserts interest in the information. The requirement that disclosure of the information must be clearly in the public interest means that the information must relate to a matter of compelling public interest, and not just be of interest or of curiosity to the public, a group of people, or individuals. What constitutes a compelling public interest is defined narrowly (*IPC Order 96-011*). The following are some examples where disclosure may clearly be in the public interest:

- a public body has been alerted about a contagious disease or about an individual who is the carrier of a contagious or dangerous disease;
- a violent or dangerous offender has been released into the community;
- an individual seeking employment in child care on the basis of a false resumé is found to have a history of child molestation that is recorded in a register of employment references for child-care workers; and
- information has come to light about corruption or serious misuse of public funds.

The following are some of the instances where the Commissioner has, in reviewing decisions under **section 32**, found that the public body was *not* required to disclose the requested information.

- A public body was not required to disclose records relating to the government's involvement in a commercial enterprise, even though the Commissioner found that this was a matter of compelling public interest. The public interest requirement had been satisfied when the Auditor General's report on the matter was publicly released (*IPC Order 99-023*).
- A public body was not required to disclose information concerning contracts with health-care service providers. The Commissioner found that, although there was public interest in the quality of health care, the information in the records requested concerned the legal interpretation of words and phrases. The applicant had not established that this particular information related to a compelling public interest (*IPC Order 2000-031*).
- A public body was not required to disclose operating manuals under a photo radar contract. The Commissioner decided that disclosure of the manuals, which the applicant argued would enable people to defend themselves in a court of law, was not clearly in the public interest (*IPC Order 2000-017*).
- A public body was not required to disclose information about the payouts and severance pays of former police chiefs. The spending of public funds does not, by itself, create a matter of public interest that overrides the exceptions in the *FOIP Act* that permit a public body to refuse disclosure (*IPC Order F2006-010*).

- A public body was not required to disclose information about the legal fees incurred by the government in proceeding with the case *Reference Re: Firearms Act*. There may be public interest in government legal bills related to the case, but the applicant failed to prove that the interest was compelling (*IPC Order F2004-017*).
- A public body was not required to disclose information relating to the charges against, and trial of, a former government official found guilty of accepting a benefit. Since the issue had been dealt with through the legal process and related court documents were available to the public, there was no compelling public interest requiring disclosure under **section 32** (*IPC Order F2004-030*).
- A public body was not required to disclose information regarding a law firm's bill for legal services provided to the public body. The information was subject to solicitor–client privilege, and the public interest in maintaining solicitor–client confidentiality outweighed the public interest in disclosing solicitor–client communications (*IPC Order F2007-014*).

Criteria applied by public bodies to determine whether a fee waiver should be granted in the public interest under **section 93(4)(b)** are not the criteria to be applied for determining whether disclosure is in the public interest under **section 32** (see *IPC Order 2000-005* and Chapter 3, section 3.5 on excusing fees).

#### **Duty to disclose information under section 32**

A public body has a duty to disclose information if **section 32** applies. If a complaint were made to the Commissioner that a public body did not disclose information in the public interest, the public body would have to show why it did not do so in that particular situation.

Public bodies may find it helpful to plan for the release of information in emergency-like situations by developing an assessment of the conditions under which **section 32** might arise, the information that might be involved, and considerations that might be relevant to the decision-making process. It is recommended that a senior official in the public body, such as a Deputy Minister or Chief Administrative Officer, retain the authority for decisions on **section 32** disclosures.

---

#### **6.4**

##### **Notification**

#### **Notification prior to disclosure**

**Section 32(3)** provides that, before disclosing information under **section 32(1)**, the public body must, if practicable,

- notify any third party to whom the information relates;
- give the third party an opportunity to make representations relating to the disclosure; and
- notify the Information and Privacy Commissioner.

Normally, notice must be given to affected third parties and the Commissioner *before* the information is released under **section 32(1)**. This obligation to notify third parties and the Commissioner must be balanced against the obligation to disclose the information without delay. Notification is to take place only where practicable, and

the head of the public body must ensure that there is no delay adversely affecting the public interest. The factors governing release without delay apply here.

Notice should take a similar form to the notice required by **section 30(1)** of the Act. Since the matter may be of some urgency, notice should be delivered by fax or courier and accompanied by a telephone call advising the third party of the importance of quickly delivering any representations they may have about the disclosure to the public body. Depending on the urgency, the third party may be asked to respond immediately or within a short period of time.

**Model Letter P** in Appendix 3 can be used in this situation.

The third party notice should be sent to any person, group of persons or organization that is a subject of the information or the record(s), other than the person who made the request or the public body involved.

A similar notice, or a copy of the one sent to the affected person together with a covering note, must be sent to the Commissioner to inform that office that a disclosure in the public interest is being made.

Public bodies that intend to disclose information in the public interest should not inappropriately disclose personal information of a third party. The amount and type of personal information that is disclosed should be limited to what is necessary to make the public or the affected group or individual sufficiently aware of the risk or danger to their health or safety or to the environment.

#### Notice of disclosure

**Section 32(4)** requires that, where notification is not practicable under **section 32(3)**, the public body must give written notice that disclosure has occurred

- to the third party, and
- to the Commissioner.

The form of the notice to be given to the third party is prescribed in **Schedule 3** of the FOIP Regulation. **Model Letter Q** in Appendix 3 meets the requirements of the Regulation and can be used in this situation. A copy of the letter and a covering note can serve as notice to the Commissioner.

#### 6.5 Review

If there is a complaint about the failure of a public body to release information in the public interest, the Information and Privacy Commissioner can review the head of the public body's decision in the following situations:

- if a FOIP request has been made, under the powers provided in **section 65(1)** of the Act, which enables an applicant to request a review of the decision and sets out the process, and
- if no FOIP request has been made, under the general powers of the Commissioner set out in **section 53(1)** of the Act, which permits an investigation of various matters relating to the legislation.

*IPC Order 96-011* discusses the powers of review and investigation of the decision of the head of a public body in dealing with disclosures under **section 32**. In that Order, the Commissioner clearly indicated that a person would have to first approach the head of a public body to request disclosure in the public interest. The Commissioner may then review or investigate a decision of the head to disclose or not to disclose information under **section 32**, but only to the extent of deciding whether discretion has been exercised properly and whether the decision is rationally defensible. The Commissioner will not substitute his view for that of the head of the public body as to whether the decision is the correct one.

In a review where an applicant argues that the public body should disclose the requested information because it is in the public interest to do so, the burden of proof is on the applicant. The applicant must prove that a matter of compelling public interest requires the public body to disclose certain information that would normally not be disclosed, for example, under **sections 16 or 17** (see *IPC Order 2000-003*). Once the applicant has met the burden, the onus shifts to the public body, which must then establish that a decision not to disclose the information is rationally defensible (*IPC Order F2006-010*).

For more information on the issue of burden of proof, refer to FOIP Bulletin No. 9: *Burden of Proof*, published by Access and Privacy, Service Alberta.

The powers of the Commissioner are discussed in more detail in Chapter 10.







## 7.

## PROTECTION OF PRIVACY

## Overview

This chapter covers the obligations of public bodies regarding

- the collection, use and disclosure of personal information;
- the accuracy of personal information;
- the retention of personal information;
- the protection of personal information; and
- the right of an individual to request a correction of his or her personal information.

## Privacy principles

The *FOIP Act* ensures the protection of informational privacy (the right to exercise control over your own personal information) by establishing rules for the collection, use, disclosure and retention of personal information. The Act also contains rules regarding the accuracy of personal information, and gives individuals the right to request a correction to their personal information in the custody or control of a public body.

Most of the provisions respecting the protection of personal information are found in **Part 2** of the Act; however personal privacy is also considered in **section 17**.

**Part 1** **Part 1** of the *FOIP Act* provides individuals with a right of access to information, including information about themselves, from public bodies, subject to limited and specific exceptions. One of those exceptions, **section 17**, sets out factors to determine when disclosure of personal information would be an unreasonable invasion of a third party's privacy. These factors come into play whenever someone other than the individual the information is about, or the individual's authorized representative, makes a request for access to a record containing personal information about a third party.

Personal information, as defined in **section 1(n)**, means recorded information about an *identifiable* individual. It is information that can identify an individual (for example, name, home address, home phone number, e-mail address, ID numbers), and information about an individual (for example, physical description, educational qualifications, blood type). An individual may be identified by their name, where they live, what they do, or as a result of a compilation of information that relates to only to a small number of people (see, for example, *IPC Investigation Report F2004-IR-001*). The definition of personal information does not include information about a sole proprietorship, partnership, unincorporated association or corporation (see *IPC Order F2002-006*).

**Part 2** Information about an identifiable individual that is collected must be collected, used, disclosed, secured, and retained only in accordance with the provisions in **Part 2**,

unless the information is outside the scope of the Act (see sections 1.5 and 1.6 of Chapter 1 regarding excluded records and the effect of paramouncy, respectively).

**Part 2** requirements are based on internationally accepted fair information practices or principles adopted by the Organization for Economic Cooperation and Development (OECD) in 1982. This set of principles collectively works to establish what is commonly referred to as *privacy protection*. An individual's privacy is protected when the individual is able to decide who to give their information to, is aware of how the information will be used and disclosed, and gives consent to use and disclose the information if appropriate.

Privacy is protected in the *FOIP Act* by

- giving individuals a right of access to their own personal information and the opportunity to request corrections to it;
- collecting personal information only as authorized by law;
- requiring public bodies to collect personal information directly from the individual the information is about, unless the individual, another Act or a regulation under another Act, the Information and Privacy Commissioner, or **section 34(1)(b) to (o)** of the *FOIP Act* authorizes collection from someone else;
- requiring public bodies to provide individuals with notice of the authority for the collection, the purposes for which the information is collected and contact information for a person who can explain the collection process in more detail, if required;
- requiring public bodies to ensure that information that will be used to make a decision about an individual is accurate and complete;
- requiring public bodies to retain information used to make decisions affecting an individual for at least one year (unless the public body and the individual agree otherwise) to allow adequate time for the individual to exercise their right of access or correction, if they choose to;
- requiring public bodies to take reasonable security precautions against such risks as unauthorized access, collection, use, disclosure or destruction;
- limiting a public body's use and disclosure of personal information to the purpose for which it was collected, a consistent purpose, another purpose with consent or a purpose set out in the Act;
- further limiting a public body's use and disclosure of personal information to the amount and type necessary to enable the public body to carry out its purpose in a reasonable manner;
- enabling individuals to make complaints to the Commissioner, and empowering the Commissioner to investigate complaints regarding possible collection, use or disclosures in contravention of **Part 2**;
- enabling employees of a public body to disclose to the Commissioner, in good faith, circumstances in which they believe that personal information is being collected, used or disclosed in contravention of **Part 2** (see section 2.9 of Chapter 2);

- requiring each public body to publish a directory of its personal information banks (repositories of personal information that can be searched by name or identifier); and
- providing for fines for individuals of up to \$10,000 if they wilfully collect, use or disclose personal information in contravention of **Part 2**, or gain, or attempt to gain, access to personal information in contravention of the Act (among other offences).

The *FOIP Act* does, however, also recognize that public bodies must collect and maintain a variety of personal information for purposes related to direct service delivery to members of the public or for broader public purposes. In some instances, authority to collect, use or disclose personal information is expressly granted in the *FOIP Act*. In others cases, the authority to collect, use or disclose personal information is granted by other enactments of Alberta or Canada.

FOIP Coordinators are advised to take a comprehensive and collaborative view of privacy protection within their public bodies and involve individuals with responsibility for program management, information technology, records and information management, security, human resources and, at times, their legal counsel. FOIP Coordinators should also be aware of other privacy legislation that governs bodies with which they interact. For example, a public body may not be able to collect personal information from a private-sector organization in Alberta if that organization is not authorized to disclose the information under the *Personal Information Protection Act* (PIPA).

Under the *FOIP Act*, public bodies are accountable for adhering to the privacy protection rules established in **Part 2**, and are accountable for ensuring that other organizations acting on behalf of the public body also adhere to these rules. It is in the public body's best interest to ensure that their obligations and requirements under the Act are clearly understood by any contractor or agent and the obligations are clearly communicated in the contractual agreement.

For further information on the application of the Act to the contracting process, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

## 7.1

### Collection of Personal Information

#### Authority for collection of personal information

Public bodies cannot collect personal information unless the collection is authorized under **section 33** of the Act. **Section 33** of the Act authorizes the collection of personal information if

- the collection of personal information is expressly authorized by or under an enactment of Alberta or Canada;
- the personal information is collected for the purposes of law enforcement; or
- the personal information relates directly to and is necessary for an operating program or activity of the public body.

*Collection* occurs when a public body gathers, acquires, receives or obtains personal information. It includes the gathering of information through forms, interviews, questionnaires, surveys, polling, and video surveillance. There is no restriction on how the information is collected. The means of collection may be writing, audio or videotaping, electronic data entry or other means.

**Section 33** of the Act states that collection can take place *by* or *for* a public body. A public body is bound by the requirements of the Act whether it conducts its own collection activities or an outside agent carries out the collection on the public body's behalf. This authorization may be either under contract or through an agreement or arrangement with another public body or private organization.

Examples of organizations and individuals that might collect personal information on behalf of a public body include non-profit support groups such as the John Howard Society, school counsellors and various contracted organizations.



When an outside organization or contractor is collecting personal information on behalf of a public body, the public body should have in place a written agreement or contract. This must state how the organization or contractor will meet the requirements of the *FOIP Act* regarding the collection, use, disclosure, security, retention and disposition of the personal information being collected.

#### **Authorized by an enactment**

**Section 33(a)** **Section 33(a)** provides that collection may be expressly authorized by an enactment of Alberta or Canada.

An *enactment* includes an Act or regulation, or any part of an Act or regulation. A municipal bylaw passed under the authority of the *Municipal Government Act* may also be considered an enactment for the purposes of **section 33(a)**. In *IPC Investigation Report F2002-IR-009*, the Investigator found that a municipal bylaw expressly authorized the City to collect criminal record information from applicants for taxi licences.

In some Acts, there are provisions for the collection of certain specific types of personal information. In these cases, the statute both authorizes collection and identifies the personal information that can be collected (e.g. section 65 of the *Post-secondary Learning Act*). More commonly, an Act will authorize a program or activity, and a regulation under that Act will provide detailed authority for collection and sometimes the format in which the information is to be collected. An example of this form of authorization for collection is the *School Act* and the Student Record Regulation. Another model for collection authority is where an Act states that collection of personal information must be in the form prescribed by a regulation under that Act.

If an enactment authorizes a program or activity, but there is no specific authorization for the collection of information for the purposes of the program or activity, a public body cannot rely on the enactment as authority for collection of the information. It is



not sufficient for an enactment to imply an ability to collect personal information (see *IPC Order F2006-004*).

If a particular collection of personal information is not authorized under **section 33(a)**, it might be authorized under **section 33(b)** or **(c)**.

***For the purposes of law enforcement***

**Section 33(b)** **Section 33(b)** permits the collection of personal information for the purposes of law enforcement. *Law enforcement* is defined in **section 1(h)** of the Act and is discussed in section 4.6 of Chapter 4. It includes policing, administrative investigations, and proceedings that could lead to a penalty or sanction. Any collection of personal information for purposes of law enforcement must meet this definition.

**Section 33(b)** recognizes that law enforcement agencies must engage in wide-ranging information collection that would not always be allowed under the more restrictive terms of **section 33(c)**. It would be difficult for a law enforcement agency to show, at the moment of collection, how each piece of personal information collected for investigative or enforcement purposes relates directly to or is necessary for the activity under way. Certain investigative methods, such as taking witness statements, might be seriously compromised by limiting the collection of personal information.

In *IPC Investigation Report F2003-IR-005*, the Information and Privacy Commissioner reviewed a Privacy Impact Assessment submitted by a police service regarding video surveillance it intended to use in an area of the city during two periods of highest crime risk. The Commissioner agreed that the police service could collect and use personal information on video for this law enforcement activity, which included the detection and prevention of crime.

If a public body is authorized to collect personal information under this provision, it is also authorized to collect the information indirectly under **section 34(1)(g)**.

For more information on collection for the purposes of law enforcement and about the definition of law enforcement, see FOIP Bulletin No.7: *Law Enforcement*, published by Access and Privacy, Service Alberta.

***Relates directly to and is necessary for an operating program or activity***

**Section 33(c)** **Section 33(c)** permits a public body to collect personal information when that information relates directly to, and is necessary for, an operating program or activity of the public body.

*Relates directly* to means that the personal information must have a direct bearing on the program or activity.

*Necessary for* means that the public body must have a demonstrable need for the information.

An *operating program* is a series of functions designed to carry out all or part of a public body's operations. An *activity* is an individual action designed to assist in carrying out an operating program.

Most often, legislation will give authority for a particular program or activity, without authorizing the collection of specific personal information. Public bodies must then determine the exact elements of personal information which they need to administer a particular program and design collection instruments to obtain this information *and no more* (i.e. the public body must have a “need to know”). Collection is authorized by **section 33(c)** of the Act.

The *FOIP Act* does not permit collection of personal information “just in case” it may have value in the future, the program may be expanded in the future or someone in the public body may ask for the information at some point in the future.

The word *and* in **section 33(c)** (relates directly to and is necessary) is restrictive. The collection must meet both parts of the two-part test in order for the public body to use **section 33(c)** as authority to collect personal information.

For example, if a program provides a particular benefit or service, information will be needed to ensure that an individual is eligible or qualified for that benefit or service. Personal information not related to decision criteria for the particular benefit or service is not required and should not be collected, even though it may be potentially useful to another program in the same public body.

In *IPC Order 98-002*, the Commissioner determined that the case manager making a decision about an individual’s claim for compensation had the right to decide what medical information was relevant and necessary to collect but was bound by the *Workers’ Compensation Act* in establishing that necessity and relevance. Obtaining an applicant’s entire patient file was found to be an improper collection.

In *IPC Investigation Report 99-IR-007*, the Commissioner found that a municipality did not have the authority to collect its Sport Centre’s members’ home or business telephone numbers or dates of birth since this information was not required for an operating program or activity of the municipality.

In *IPC Investigation Report F2002-IR-010*, the Investigator found that using one questionnaire to collect personal information for two programs risked collecting more personal information than was necessary for the public body’s operating program or activity. In this case, the survey was completed by both current and prospective employees, although only one of the programs applied to prospective employees. The survey collected more personal information from the prospective employees than the public body required.

A public body must establish a reasonable basis for deciding that the collection of personal information is necessary and relevant. The City of Calgary Fire Department provided sufficient evidence to show that the sensitive personal information collected during its recruitment process was relevant to job requirements, based on findings from research and potential conflict situations that a firefighter might encounter. (see *IPC Investigation Report F2002-IR-012*).

The manner in which information is collected should be minimally intrusive. Collecting information about employees through surreptitious keystroke-logging technology did not meet the “necessary” requirement since there was other less

intrusive means of collecting information about employee productivity (see *IPC Order F2005-003*).

A determination about what personal information is related directly to and necessary to collect would likely be overturned only if it was patently unreasonable (see *IPC Investigation Report F2002-IR-012*).

### Review of collection practices

A public body should regularly review their collection practices to ensure that any collection of personal information is authorized by **section 33**. Such a review should

- verify that there is authority for the collection of personal information;
- discontinue the collection of personal information that does not meet the criteria set out in **section 33** and amend forms and other collection instruments, contracts and agreements, and policies and procedures that require the collection of this personal information (for more information on reviewing collection instruments, see section 9.4 of Chapter 9);
- confirm that a process is in place to ensure that all new or modified collections of personal information meet the criteria set out in **section 33** and ensure that the minimum personal information necessary to meet program needs is collected;
- ensure that information that is needed only for subsets of clients is collected only from the clients that fit the subset criteria (see *IPC Investigation Report 98-IR-003*);
- verify that procedures are in place to ensure that any irrelevant personal information that is sent to a public body is placed in a separate file so that it is not improperly used, and that it is destroyed, redirected or returned to the originator at an appropriate time after completion of the process during which the information was inadvertently collected (see *IPC Order 98-002*); and
- ensure that personal information in the custody or under the control of the public body is scheduled for retention (if the information is still needed) or for deletion or destruction and that retrieval mechanisms are deactivated (if the information is no longer needed).

This review could be carried out by the program areas having custody or control over personal information, with the advice of the FOIP Coordinator.

Administrative controls should be established in privacy policies. New collection activities and instruments should be reviewed by the FOIP Coordinator's office. The review may be carried out in conjunction with reviews of information management practices and systems, which are discussed in Chapter 9.

### Unsolicited Information

If a public body does not have specific authority to collect unsolicited personal information and the information is not necessary for an operating program or activity of that public body, it is not an authorized collection (see *IPC Order 98-002*). The public body should adopt a policy of either returning the unsolicited information or destroying it in accordance with a transitory records schedule.

For example, when the Calgary Police Commission requested the names and positions of board members from the Calgary Police Association, the Association also sent the members' home addresses and telephone numbers. Since the Commission did not need this additional information, the investigating officer recommended that it be returned to the Association, and that the Commission adopt a policy that all unsolicited information be returned (*IPC Investigation Report 2000-IR-002*).

In some cases, a public body might keep unsolicited personal information for a specified period of time before destroying it (e.g. unsolicited résumés). The public body should keep the unsolicited information separate from other files so that it will not be improperly used or disclosed.

## 7.2

### Manner of Collection

#### Direct collection

**Section 34(1)** states that, subject to some limited exceptions, a public body must collect personal information directly from the individual the information is about. This establishes direct collection as the primary method for obtaining personal information. This is an important principle for fair information practices. It helps to ensure that an individual is aware of the type of personal information being used to make a decision concerning him or her. It also allows the individual to challenge the need for the information or refuse to provide the information or participate in the program or activity. Collecting information directly from the individual it is about will generally fulfil a public body's requirement to make every reasonable effort to ensure that the personal information is accurate and complete (for further information on accuracy and completeness, see section 7.3 of this chapter).

A public body must not seek or passively receive the information from another source even though it may have the capability of doing so, unless collection from that indirect source or for that purpose is authorized in the exceptions listed under **section 34(1)**.

#### Exceptions to direct collection

The Act provides for circumstances where personal information about an identifiable individual may be sought from sources other than the individual the information is about. If one of the provisions in **section 34(1)** applies, personal information may be obtained in verbal, written, electronic or other form (e.g. a file transfer).

#### Another method of collection is authorized

**Section 34(1)(a)** This provision allows a public body to collect personal information about an individual from another public body, or other individual or organization under one of the specified conditions.

**By the individual.** When an individual authorizes the collection of his or her personal information from another source, as in the case of a student requesting a reference from a professor, this authorization should be in writing. This may take the form of a signed authorization on an application form or a letter giving authorization. If an individual provides authorization orally over the telephone, the public body

should document the conversation and, whenever possible, send a letter to the individual concerned setting out what he or she has authorized.

When asked to authorize indirect collection of personal information under **section 34(1)(a)(i)**, the person should be informed of

- the nature of the personal information to be collected (i.e. how much of what type of information is being collected);
- the purpose of the indirect collection (i.e. what the information will be used for);
- the reasons for making the collection indirectly;
- the identity of the recipient and the expiry date of the authorization, and
- the consequences of refusing to authorize the indirect collection.

If an individual authorizes a public body to collect personal information from another public body or from a custodian under the *Health Information Act*, the written authorization for the collection is often included in the same form as the authority for the other body or custodian to disclose the necessary information to the first public body. As a result, the authorization format should take into consideration the disclosure (and possibly the consent) requirements of the *FOIP Act* and the *Health Information Act* if the disclosing public body is a custodian under that Act.

**By another Act or a regulation under another Act.** Sometimes another Act or regulation under another Act specifically authorizes indirect collection of personal information. For example, the *Workers' Compensation Act* authorizes collection of medical information from a physician about an individual who was involved in a work-related accident.

Another example is the Student Record Regulation, which authorizes public schools to collect teachers' notes about students and other personal information in records from a student's previous private school (see *IPC Order 2001-034* and *IPC Investigation Report F2002-IR-007*).

**By the Information and Privacy Commissioner.** The Commissioner has the power to authorize indirect collection under **section 53(1)(h)**. This provision addresses situations where indirect collection should be considered but **section 34** does not permit it. The Commissioner has the responsibility of deciding how and under what circumstances he will exercise the power.

#### **Information may be disclosed under Division 2 of Part 2 of the Act**

**Section 34(1)(b)** This provision permits a public body to collect personal information from a second public body, rather than from the individual the personal information is about, where the second body is authorized to disclose the information under **sections 40 to 42** of the Act.

**Part 2** of the Act is structured in such a way that if a public body is authorized to disclose certain personal information to another public body, the receiving public body is, in turn, authorized to collect the information and to use it for the purpose for which it was disclosed.





Where public bodies rely upon section 34(1)(b) to collect personal information indirectly, the public body that has the information must be satisfied that the disclosure is authorized. The public body receiving the information must ensure that it is authorized to collect it under section 33.

This provision permits disclosure of personal information by one public body to another in limited and controlled circumstances.

***Information is collected in a health or safety emergency***

**Section 34(1)(c)** This provision allows emergency services personnel, as well as other employees of a public body, to collect information needed to deal with an emergency situation.

This can happen when

- the individual is not able to provide the information directly; or
- direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person.

Examples of such emergency situations include cases where an injured person is not able to respond to questions about medication or an accident or fire situation when a delay in collecting information about a person's actions could result in death or severe complications.

Under this provision, a public body can collect indirectly only the information required to deal with the emergency.

***Information is about a designated emergency contact***

**Section 34(1)(d)** This provision allows for the collection of contact information such as a name, relationship, address and telephone number(s). The individual may be a family member or a friend. This is the personal information of the contact and this information would be collected from an individual who is required to provide an emergency contact.

Such information is often provided when, for example, students enter a college residence, children are registered in a day camp program or for a school field trip, or a public body hires a new employee.

***Information is collected to determine suitability for an honour or award***

**Section 34(1)(e)** This provision allows a public body to seek references and other relevant personal information about someone being considered for an honour or award. This includes honorary degrees, scholarships, prizes, and bursaries.

The nature of some awards is such that the potential recipients do not have to apply for the award and may not be aware that they are being considered. Scholarships and bursaries are often awarded on the basis of academic achievement and recommendations by faculty members. Honorary degrees are usually awarded in recognition of a person's contribution to a community or sector of society. Prizes may be awarded on the basis of athletic or scholastic achievements.

Any information collected should be directly related to the criteria for granting the honour or award. As a best practice, public bodies should develop criteria for an award in advance of the collection of personal information about award nominees and make those criteria generally available. Once the individual has been informed about the honour or award, his or her personal information should only be disclosed with consent, unless another exception for disclosure applies.

***Information is collected from published or other public sources for fund-raising***

**Section 34(1)(f)** This provision allows for limited collection of publicly available personal information without the authorization or knowledge of an individual. The information collected can be used only for fund-raising purposes. Public bodies should keep such information segregated in their records and allow access by only those employees engaged in fund-raising and fund development activities.

*Published sources* are publishers, including a company that produces and distributes books and newspapers, but also by a publisher that distributes information only in electronic form, most commonly on a website. Examples include newspaper reports, clipping files, corporate reports of public companies, and articles in periodicals. Most of this information would be readily available in a public or specialized library.

*Other public sources* includes information that is made available to the public at large in any medium. The information may not be routinely made available; it may be of a kind that can be made available on demand, for example, through a search of a database or making a request for a public record, as in the case of certain classes of court records. The information may be made available free or for a fee. Examples include information in reports of charitable organizations, announcements of honours or awards granted by or through a public body in Alberta, copies of speeches or speaking notes when the speeches are given at a public event, and information available on the Internet. Care should be taken when relying on personal information that is collected from the Internet; the credibility of the source of the information should be considered. The public body should also bear in mind that this personal information would be accessible to the individual if he or she made an access request.

Not included under this provision is information of a more private character, such as information based on personal acquaintance, friendship or observation that may be provided by members of a governing board or employees; information that could only be gathered through surveillance or from private sources; next-of-kin information; and names of parents of students. For more information on this provision, see FOIP Bulletin No. 5: *Fund-Raising*, published by Access and Privacy, Service Alberta.

***Information is collected for the purpose of law enforcement***

**Section 34(1)(g)** This provision allows the indirect collection for law enforcement activities as defined in **section 1(h)** of the Act, including policing and investigations.

It should be noted that the authority to collect personal information under **section 34(1)(g)** is limited. Under the definition of law enforcement in **section 1(h)**, as interpreted by the Commissioner, the law enforcement body must ensure that there is a specific authority to investigate and that the investigation could lead to a penalty or

sanction being imposed under a statute or regulation. See section 4.6 of Chapter 4 for information on the definition of law enforcement.

Much personal information about a person who is under investigation is collected from other sources. Reasons for this include the fact that investigators may not wish to alert the individual concerned that an investigation is taking place, the individual would not provide accurate information, or the individual might alter or destroy evidence. Disclosure of personal information by private-sector organizations in Alberta is governed by the *Personal Information Protection Act* (PIPA), or in some cases, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Law enforcement bodies may wish to refer to the *Requesting Personal Information from the Private Sector: A Guide for Law Enforcement Agencies*, published by Access and Privacy, Service Alberta.

Law enforcement bodies should not collect excessive amounts of personal information. One of the situations where this is likely to occur is in the use of surveillance. The Commissioner considered the use of video surveillance for law enforcement purposes in *IPC Investigation Report F2003-IR-005*.

***Information is collected for the purpose of collecting a fine or debt***

**Section 34(1)(h)** When public bodies face the problem of not being able to locate those owing money, or when they believe they would not obtain accurate information needed to collect the debt from the individual debtor, they are permitted to collect personal information from other sources.

This provision allows a representative of either the provincial government, as a whole, or any individual public body to contact any person or organization or to use publicly available information (e.g. on the Internet) that may be able to help in the collection of money owed to the public body or the government. This may include finding the home or work location or telephone number of the individual who owes money.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

A *fine* is a monetary punishment imposed on a person who has committed an offence, including an offence under a bylaw.

***Information concerns the history, release or supervision of an individual under the control of a correctional authority***

**Section 34(1)(i)** This provision permits correctional and parole authorities to seek out information from a variety of sources about individuals under their control or supervision. The individual may be in a correctional institution or may be under supervision in the community.

If a community service organization is itself a public body, or is under contract to a public body to provide services to individuals under the control or supervision of a correctional or parole authority, it may rely on **section 34(1)(i)** for indirect collection of personal information about the individual's history, release or supervision relevant to the service being provided.

*History* here means information about the person's background, including employment record, medical condition and behaviour.

*Release* includes both permanent and temporary release from a correctional institution.

*Supervision* includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of an individual held in a correctional institution.

***Information is collected for use in the provision of legal services to the Government of Alberta or a public body***

*Section 34(1)(j)* This provision permits that lawyers representing the provincial government or a public body may have to collect personal information to perform their jobs. The information may be required for day-to-day provision of legal services, or in preparation for a proceeding before a court or tribunal.

It is often not possible to collect the personal information directly because inaccurate information may be given. It may also be desirable that legal enquiries be made in confidence, or it may be that the individual concerned may not be able to provide the required information. In these circumstances the public body's legal representatives, or others providing legal services, can collect information indirectly, or ask an employee to do so on their behalf.

***Information is necessary to determine eligibility to participate in a program or receive a benefit, product or service***

*Section 34(1)(k)(i)* Many programs operated by public bodies have eligibility criteria that must be met in order for an individual to participate in them or receive a benefit or service. This may require the public body to approach several different sources of information besides the individual to determine whether the criteria or qualifications are met. Examples include verification of income for the Alberta Seniors Benefit, low-income housing or other income-tested programs; verification of assets for programs requiring asset testing; and verification of educational prerequisites for a post-secondary program.

This collection of information can take place only in the course of processing an application from the individual, or from his or her representative. It is a good business practice to inform the individual about whom information is being collected that information from a variety of sources will be collected to document a particular application. Public bodies should not take the further step of asking an individual to authorize indirect collection unless they are prepared to modify their procedures for determining eligibility if an individual refuses to authorize the indirect collection. Authorization from the individual is not necessary if the requirements of **section 34(1)(g)** are fulfilled.

***Information is necessary to verify eligibility to participate in a program or receive a benefit, product or service***

*Section 34(1)(k)(ii)* This provision is intended to allow for cases where an individual has already qualified for a program, benefit, product, or service and the public body needs to check that the individual is still eligible. In this case, personal information may be

collected from a variety of sources other than the individual the information is about, and the individual does not need to be informed that verification is taking place.

For example, a public body may perform random checks on the income and assets of individuals on social assistance or in low-income housing to verify that an individual remains eligible for the program. Such a check may involve an interview with the individual but may also involve collection of personal information about an individual from other sources. Another example would be verification of a student's continued enrolment in a program so that the student may continue to receive student financial assistance or a grant.

As with the previous provision, it is a good business practice to inform the individual about whom the information may be collected that verification of continuing eligibility may occur without notice. This is especially the case if the individual could incur any penalty for receiving a benefit for which he or she has become ineligible.

***Information is collected by the Public Trustee or the Public Guardian***

**Section 34(1)(l)** The *Public Trustee* is the trustee for dependent adults who are unable to administer their own financial affairs because of a mental disability. The Trustee also administers the estates of persons who die intestate if the deceased persons have no adult beneficiaries residing in the province. In addition, the Trustee acts as guardian by protecting the assets and financial interests of missing persons and children under 18 years of age.

The *Public Guardian* is charged with the responsibility of ensuring that appropriate surrogate decision-making mechanisms, supports and safeguards are available to assist adults who are unable to make personal decisions independently.

**Section 34(1)(l)** permits the Public Trustee and the Public Guardian to collect personal information about a prospective ward indirectly from relatives, friends and others. This may include information about the individual's mental or physical health, financial information, employment or educational history, and opinions about the individual.

Under the *Public Trustee Act*, section 44, the Public Trustee may compel a person, including a public body, that has possession of personal, financial or health-related information about a client or potential client, to provide that information or record to the Public Trustee for the Public Trustee to carry out a task, duty or function relating directly to the client or prospective client.

***Information is collected for the purpose of enforcing a maintenance order***

**Section 34(1)(m)** This provision permits Alberta Justice and Attorney General to collect personal information for the purpose of enforcing maintenance orders.

Amendments to section 12 and section 13 of the *Maintenance Enforcement Act* require government departments, provincial agencies (e.g. post-secondary institutions) as well as business organizations (including municipalities) to provide an expanded number of types of personal information (e.g. financial information, an identification number issued by a province) to the Director of Maintenance Enforcement for the purpose of enforcing a maintenance order. Only the requested



information that is listed in that Act should be disclosed by a public body and collected by the Director.

***Information is collected to manage or administer personnel of the public body***

**Section 34(1)(n)** This provision permits the Government of Alberta as the employer for all provincial government departments. It allows government departments to collect personal information about an employee or prospective employee from other provincial government departments for the purpose of managing or administering personnel of the Government of Alberta.

*Management of personnel* refers to aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees (see *IPC Investigation Report 2001-IR-006*). This includes staffing requirements, job classification or compensation, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training and development, occupational health and safety, and separation and layoff. For the Government of Alberta, the term includes the government-wide network managed through the Corporate Human Resources. It does not, however, include the management of consultant, professional or independent contractor contracts.

*Administration of personnel* comprises all aspects of a public body's internal management, other than personnel management, necessary to support the delivery of programs and services. Administration includes business planning, financial, materiel, contracts, property, information, and risk management (see *IPC Investigation Report 2001-IR-006*).

**Section 34(1)(n)** also allows public bodies to collect information about employees or prospective employees from third parties. Any collection under this provision must have, as its purpose, the management or administration of the personnel of the public body collecting the information.

Employees should be informed in a general way as to how personnel information about them is collected and from what sources they can expect this information to be derived. They should also be aware of the purposes for which various types of information are used and of their rights under the Act.

Examples of such collection include the collection of references for prospective employees, determination of qualifications and performance for secondment and training opportunities, and the provision of pay and benefit services by one public body for other public bodies.



**Section 34(1)(n) refers to official personnel activities and does not permit the collection of personnel-related information by individual officials for purposes other than official duties relating to the management and administration of personnel within a public body.**

The indirect collection authorized in **section 34(1)(n)** does not apply to other internal activities of public bodies, such as Corporate Challenge events and United Way

campaigns. Personal information of employees not related to managing or administering personnel should be collected directly from the individuals and the notification provisions in **section 34(2)** need to be complied with.

***Information is collected to assist in researching or validating the claims, disputes or grievances of aboriginal people***

**Section 34(1)(o)** This provision permits a public body to collect personal information indirectly in order to research the background of the claims, disputes or grievances and expedite the settlement of wider rights of aboriginal people.

*Validating* means confirming rights that have been contended by the parties to a claim, dispute or grievance.

The term *claims, disputes and grievances* is interpreted broadly to include all manner of controversies, debates and differences of opinion regarding issues in contention and is not restricted to differences over land claims.

*Aboriginal people* means individuals whose racial origins are indigenous to Canada, including Indian, Métis and Inuit people.

**Notification**

**Section 34(2)** **Section 34(2)** sets out rules that a public body must follow when it is required to collect personal information directly from an individual. The notification requirement allows an individual to know the purpose of the collection of personal information and how the information will be used.

A public body must inform the individual of

- the purpose for which the information is collected;
- the specific legal authority for the collection; and
- the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

The *purpose* of a collection means the reason(s) the information is needed and the use(s) that the public body will make of the personal information.

The *legal authority* for collection may be a specific provision in an enactment of Alberta or Canada that expressly authorizes collection of the personal information, or **section 33(c)** of the *FOIP Act*, which authorizes collection of personal information that is directly related to and necessary for an operating program of a public body.

If a public body relies on **section 33(c)** of the *FOIP Act*, it is important to also provide the authority for the program for which the personal information is being collected. The program itself may be authorized by an Alberta or federal Act or a regulation under an Act, or a bylaw or legal resolution of a public body establishing a program that falls within its mandate under an Act.

Identifying someone to answer the individual's questions about the collection is intended to provide the individual with a knowledgeable source of information. The

person cited should be familiar with the program, and be able to explain why the personal information is being collected and how it will be used by, and disclosed to, other bodies.

Examples of cases where collection of personal information requires notification under this provision include collection of personal information for enrolment in a program, to receive a service or to apply for a benefit, collection of personal information on a client survey and collection of individually identifying information on a course evaluation form.

Where a public body would be permitted to collect personal information indirectly but chooses to collect directly from the individual the information is about, notification is still mandatory, even if it would not be required had the public body collected the information indirectly (see *IPC Order F2006-019*).

Notification may be given in many ways. It may be

- printed on a collection form;
- contained on a separate sheet or in a brochure accompanying a form;
- presented in a pop-up window linked to an online form;
- published in a calendar of a post-secondary institution or an information brochure about a program that is provided to all applicants;
- displayed on a notice hung on the wall or placed on a service counter; or
- given orally, for example, during a phone call.

Regardless of the manner in which notification is provided, all three parts of the notice must be provided to the individual (see *IPC Investigation Report 2000-IR-004*).

The notice should be given at the time that the personal information is being collected. In *IPC Investigation Report 2000-IR-007*, the Commissioner found that a school should have provided students or parents with a notification statement when school photographs were being taken rather than during the registration process since the collection of student photographs was not part of registration.

Notice should be given to individuals at the beginning of an interview when an individual is being asked to provide his or her own personal information. If the interview is being recorded, it is good practice to record the notice at the beginning of the tape.

When a notification is given orally, either in person or over the telephone, it is a good practice to refer the individual to a written copy of the notice or to provide a printed copy either at the counter or later by mail, and to retain a record that the notice was given.

When individuals are applying for and participating in extensive and complementary programs, it may be convenient and effective to place a notice explaining all collections of personal information relating to the programs in a publication about the programs, or explain orally.

Public bodies should undertake a regular review of their collection instruments to determine which ones require the inclusion of collection notices. Collection notices should be included on all print and electronic forms used to collect personal information directly. This should be done in conjunction with the review discussed in section 7.1 of this chapter and any privacy compliance audit or forms review process, as discussed in Chapter 9.



When collection of personal information is carried out by one public body for or on behalf of another public body, this must be done under a written agreement. The agreement should state the reasons for collecting information through an agent, the specific authority for the collection, and the purposes for which the personal information will be used or disclosed. Any use or disclosure of the personal information must be authorized under the *FOIP Act*.

### Exception to notification

**Section 34(3)** provides that the requirements for collecting personal information directly and giving notice may be set aside if, in the opinion of the head of the public body, compliance with these provisions could reasonably be expected to result in the collection of inaccurate information.

*Inaccurate information* is incorrect, incomplete or misleading information, or information which does not reflect the truth.

This provision recognizes that in certain limited circumstances, such as the conduct of some surveys seeking opinions and in some psychological testing, there may be difficulty in getting accurate information if individuals are informed in advance of the reasons for the collection. In some cases, notifying individuals of the purpose of a survey would lead to responses that would distort the results.



**This provision should be used only in limited circumstances within programs, and public bodies should maintain documentation of when the provision has been used and the reasons for using it.**

### 7.3 Accuracy and Retention

**Section 35** of the Act provides that, if a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must

- make every reasonable effort to ensure that the information is accurate and complete; and
- retain the personal information for at least one year after using it so that the individual has an opportunity to obtain access to it.

Retention may be for a shorter time period under certain conditions discussed below in relation to **section 35(b)** of the Act.

*A decision that directly affects the individual* is one that has an impact on an individual's life or affects his or her rights. The meaning of the term is interpreted broadly and includes decision-making processes that are internal to a public body and those which involve a more direct relationship with the public.

Examples of decisions that directly affect an individual include a determination as to whether or not someone is entitled to income assistance or a student loan, a decision on hiring an individual or on admission to a course or program, and a determination regarding eligibility for subsidized housing or library services.

**Section 35** does not apply if no decision, adverse or otherwise, will be or has been made about an individual. Examples include raw survey data where personal information is collected but the results are rendered anonymous, telephone messages, and unsolicited résumés that are never considered in relation to a position.

### **Accuracy and completeness**

*Section 35(a)* **Section 35(a)** requires the public body to make every reasonable effort to ensure that personal information is accurate and complete.

A public body makes *every reasonable effort* when it is thorough and comprehensive in identifying practicable means to assure that personal information used to make a particular decision affecting the individual is accurate and complete.

*Accurate* means careful, precise, lacking errors.

*Complete* means including every item or element; without omissions or deficiencies; not lacking in any element or particular. Information is *complete* when all the information necessary to make the decision, and only the information that will be used for that purpose, is collected.

Generally, if a public body collects personal information directly, it is likely to meet the requirement of making every reasonable effort to ensure that information is accurate and complete. This is especially so if the individual has signed a statement indicating that the information is accurate and complete. However, the burden of making every reasonable effort is higher when the consequences of a decision are greater.

Public bodies should have adequate procedures in place to properly verify the accuracy and completeness of any personal information crucial to an application, transaction or action at the time the information is provided (see *IPC Orders 98-002* and *2001-004*).

It is a good business practice for programs that use large personal information systems for delivery of programs or services to have systematic processes for updating personal information that is used on a regular or continuous basis.

Other methods of maintaining accuracy include periodically auditing files with accuracy and completeness as one of the criteria tested; ensuring limited access to information for the purpose of making corrections; and establishing cross-referencing and validation checks within the software of automated systems that identify



anomalies in data. Privacy requirements should be integrated into normal information and systems operations for the program as a whole.

Maintaining ongoing accuracy will be more challenging for programs that involve a lengthy review or approval process or an ongoing relationship with an individual. The accuracy requirements of the Act should be considered in the management of programs of this kind.

The Information and Privacy Commissioner has said that ensuring accuracy includes making certain that handwritten information used to make decisions, such as clinical notes, is legible (see *IPC Order 98-002*).

In *IPC Order F2003-008*, the Commissioner determined that the requirement to ensure accuracy and completeness does not apply to a reference provided by a former employee after that employee has left the employment of the public body.

### **Retention**

**Section 35(b)** This provision requires public bodies to retain personal information for at least one year after using it to make a decision that affects an individual, so that the individual has a reasonable opportunity to obtain access to it.

This retention requirement is intended to permit individuals to review and, if necessary, to request correction of information about them that has been used by public bodies, and to do so before disposition of that information takes place. It is not necessary to retain personal information when no decision will be or has been made about the individual.

*Retain* means to maintain custody or control of the personal information.

**Section 35(b)** does not prevent public bodies from storing personal information in another location, such as the Alberta Records Centre, if the public body can retrieve the personal information in response to a request for access to it.

**Section 35(b)** does not include personal information in transitory records if the information is transferred to a different format. This may be the case with records such as counselling notes or notes of an interview panel member that are consolidated into a final document, if it is the policy of the public body to treat these notes as transitory records. (See section 8.5 of Chapter 8 for further discussion of transitory records.)



**Section 35(b) overrides all records retention and disposition schedules by establishing a retention period of at least one year after use for personal information used in administrative decision-making.**

An exception to this requirement is allowed when a public body and the individual the information is about both agree in writing to a shorter retention period. In the case of government departments and agencies subject to the Records Management Regulation, a decision not to retain the personal information requires additional

approval from the Alberta Records Management Committee. This provision might be used, for example, to permit destruction of a person's application for counselling or addiction treatment when the applicant withdraws the application and does not seek the treatment. A provision in a collective agreement permitting the destruction of certain appeal hearing records within six weeks of the hearing decision satisfied the requirements for a written agreement under this section (*IPC Order F2004-027*).



**If a public body receives a request for access to personal information during the one-year retention period, the public body must keep that personal information with the request file for a further year after the last action is taken in regard to the request.**

If the Commissioner conducts a review of the response to an access request that contains personal information, the information must be retained for a year from the date that the public body complies with an order by the Commissioner to disclose the personal information.

Public bodies may keep personal information longer than one year, depending on their operational needs and on legal requirements. However, keeping personal information longer than necessary increases the risk of a security breach and of "function creep" (i.e. using the information for purposes that were not originally contemplated). Also, if the information was collected for a certain purpose and the purpose has been met, the finality principle of fair information practices suggests that the public body should then destroy it. Personal information can also be rendered non-identifying or anonymous and then retained longer for statistical purposes.

To help ensure that out-of-date and incomplete personal information is not incorrectly used in a decision affecting an individual, personal information should be scheduled for retention and disposition in accordance with the appropriate authorities for the management of recorded information.



**For public bodies subject to the *Government Organization Act*, retention and disposition of personal information must be in accordance with policies and procedures established under the *Government Organization Act* and the *Records Management Regulation*. Local public bodies must comply with legal instruments governing the retention and disposition of their records (section 3(e)(ii)).**

#### 7.4

#### Correction of Personal Information

#### Right to request correction of personal information

Under **section 36(1)**, an individual who believes that his or her personal information, in the custody or under the control of a public body, contains an error or omission may request the public body to correct the individual's personal information.

An *error* is mistaken or wrong information or information that does not reflect the true state of affairs. An *omission* is information that is incomplete or missing or that has been overlooked.

Information is personal information if it meets the definition of *personal information* in **section 1(n)** of the Act, regardless of whether the public body created or gathered the information directly or obtained it from someone else (see *IPC Order 98-001*). A public body has *custody* of a record when the record is in the possession of the public body. A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. See section 1.4 of Chapter 1 for a detailed discussion of custody and control.

In order to request a correction of personal information, an individual does not have to first make a request for access to his or her personal information. For example, a public body may refer to information contained in a record and the individual may challenge the accuracy of that record without having seen it.

A request for correction may be generated as a result of an adverse administrative decision (e.g. a denial of a claim or benefit). The *FOIP Act* does not require the public body that made the decision to revisit that decision as a result of the request.

The Act gives individuals the right to *request* a correction of personal information, not a right to have a correction made. The public body may either correct the information, by changing it or adding new information, or may refuse to correct the information, subject to other provisions discussed below.

When considering requests for correction of personal information, it is important to distinguish between the two types of information addressed by **section 36**:

- *factual information* about the applicant, such as age, date of birth, income information or qualifications (**section 36(1)**); and
- *opinions* about the applicant, such as subjective assessments or evaluations of an individual's condition, abilities or performance (**section 36(2)**).

The individual must provide proof in support of the request for correction of factual information. The proof should be of the same nature and at least the same quality as the personal information required when the original collection took place. Examples of documents that might be required to prove facts include a birth or baptismal certificate to prove age, or a notice of assessment from the Canada Revenue Agency to prove income.

Factual information does not need to be corrected if the facts are in dispute and it is not possible to make a factual determination about the issue through the inquiry process (see *IPC Orders 97-020* and *F2005-008*).

A public body must not correct an opinion (**section 36(2)**) including a professional or expert opinion (see *IPC Orders 98-010* and *2000-007*). The significance of an opinion may be that it reflects another person's view at the time it was offered, and it may be important to have a record of that view at a later date. The Act allows an

individual to have his or her views about that opinion added to the record for other readers to consider.

Although a public body cannot correct an opinion, it may, in some circumstances, seek or accept another opinion about the applicant and reconsider any decision based on the original opinion. However, the question of what information is used by a public body to make a decision about an individual is outside the scope of the Act and outside the jurisdiction of the Information and Privacy Commissioner (see *IPC Order 2001-004*).

### **How a request is made**

In many cases, an individual will ask for personal information to be corrected and supply proof of correction without doing this in a formal way. Public bodies can, and most often will, make corrections without a request under the Act if this is practical and expedites public business.

Where, in the opinion of the individual, an error or omission exists, a request for correction can be made to the public body in the form of a letter or on a **Request to Correct Personal Information Form**, a sample of which is included in Appendix 5.

Requests for correction are subject to the same rules as requests for access under the Act. This includes time limits. It also includes a duty on the part of the public body to seek clarification of a correction request, if necessary (see *IPC Order 98-010*). The Commissioner has the power to review the actions of a public body with respect to requests for correction of personal information.

### **When a correction is made**

When a public body decides to correct an error, all records containing the personal information must be corrected. This includes records in all information systems – paper, electronic and microform. Similarly, when a public body decides to add omitted information, all systems must be updated. The record should be annotated with the date of the correction. A linking mechanism, as described below, may have to be employed when personal information is stored on a medium such as microform, which may be more difficult to update.

To *annotate* personal information means to add the requested correction to the original record, close to the information under challenge by the applicant. An annotation should be signed and dated. When designing electronic forms and databases, provision should be made for allowing annotation. (For a discussion of annotation, see *IPC Order 97-020*.)

To *link* a record means to attach, join or connect the record to the requested correction. This may consist of a letter or statement from the applicant, or a copy of the **Request to Correct Personal Information Form**.

### When a correction is refused

**Section 36(3)** **Section 36(3)** provides that, when a correction is refused or cannot be made, the public body must annotate or link the personal information with that part of the requested correction which is relevant and material to the record in question.

*Relevant and material* means that there is a direct connection between the correction requested and the use that has been or may be made of the personal information and that the correction is substantive. The correction should be both pertinent to the subject matter and significant in its content.

A public body may refuse or be unable to make a correction that an applicant requests. This may be because the information is not personal information, the applicant has not submitted adequate proof in support of the requested correction, or the information consists of an opinion rather than fact (see *IPC Orders 98-010* and *2000-007*).

In the case of factual information, when the public body is not satisfied with the proof presented, the public body does not change the information but rather annotates it or links the presented information to the original information.

In the case of an opinion, a public body may describe the information in dispute and place this description, along with a statement that the applicant does not agree with the opinion or interpretation, on the record. If practicable, the applicant's request for correction may be attached (see *IPC Order 97-020*).

A public body is required to note only that part of the requested correction which is relevant to the record being annotated or to which the link is being made. Public bodies must not place the applicant's entire request on the record if it contains material that is not germane to the use made of the record (see *IPC Order F2006-017*).

### Annotating a request for correction

A model **Annotation to Personal Information Form** is provided in Appendix 5. A public body may use this form to set out an annotation relating to a correction that was requested but not made. This form clearly indicates to users that the information has been linked to a correction request and not corrected. It is filed with, or linked to, the information for which a correction was sought.



A copy of this **Annotation to Personal Information Form** or equivalent documentation must be sent to the individual requesting a correction at the time the individual is informed that the correction is not being made (see **Model Letter T** in Appendix 3). Any further information supplied by the individual after receiving this notice must be filed with the **Annotation to Personal Information Form**. (See *IPC Order 97-020*.)



In *IPC Investigation Report 2000-IR-006*, the Commissioner recommended that a municipality put a system in place that would ensure that a corrected copy of a record of personal information is sent to the individual within 30 days of a correction being made to the individual's personal information.

If the **Annotation to Personal Information Form** or the **Request to Correct Personal Information Form** cannot be physically attached to the record, a flag may be placed in the file or system containing the personal information in dispute. This will refer a user to a separate file, containing the actual disputed personal information, and indicating that a request for correction or addition of information was made but not granted.



When a public body makes an annotation or linkage regarding a request for correction that has been refused or regarding a request for correction that has been agreed upon, it must ensure that the new information is stored with the original information and will be retrieved whenever the information in question is used for an administrative purpose directly affecting the individual involved. Annotations must be made available to all users of the file or the information, including the individual, should he or she request access to his or her personal information.

In *IPC Order 2001-009*, the Commissioner found that the public body had not correctly annotated a request for correction of a videotape. Although the public body had placed the **Annotation to Personal Information Form** (see Appendix 5) on the individual's claim file, it was also required to note on the videotape label that a correction request was on the individual's file.

In *IPC Order F2003-019*, the Commissioner determined that a proper linkage was not formed when the public body simply placed the request for correction in the individual's file that contained a large number of records. The public body was required to link the request for correction to the records in question in such a manner that it would be readily apparent that a request for correction had been made for those specific records.

### Notification of other public bodies and third parties

**Section 36(4)** obliges public bodies to inform other public bodies, groups of persons, persons, or organizations that have received an individual's personal information of the request for correction or annotation of that information. Notification is required if the personal information has been shared in the year prior to the request for correction.

The notification process ensures that other parties have accurate and complete information for their own decision-making processes. In order to fulfil the notification requirements of **section 36**, a public body should keep a record of non-

routine disclosures of personal information so that if there is a request for correction the public body can inform the persons the information was disclosed to.

*Section 36(5)* **Section 36(5)** provides that such notification is not necessary if

- the correction, annotation or linkage is not material; and
- the individual who requested the correction is advised and agrees in writing that notification is not necessary.

This provision recognizes that individuals may request correction of errors in a record that are not significant for the use of the record. Public bodies may dispense with third party or public body notification if the correction requested is not required for their decision-making, provided the individual agrees with this option.



**Consent in writing from the individual is required to dispense with notification.**

*Section 36(6)* **Section 36(6)** provides that other public bodies, once notified, must make any correction, annotation or linkage to the relevant personal information disclosed to them and which is in their custody or under their control. This helps ensure that all personal information disclosed by one public body to another is accurate and complete.

#### **Time limits**

*Section 36(7)* **Section 36(7)** provides that a public body must, within 30 days of receiving the request, give written notice to the individual that either the correction has been made or an annotation or linkage has been made. It is good practice to ensure that other public bodies or third parties are also notified within the 30-day time period.

A public body may extend the time limit to deal with a request for correction for up to 30 days or, with the permission of the Commissioner, for a longer period.

**Section 14** of the Act governs these extensions; the most likely provisions to apply in correction situations are

- the applicant does not give enough detail to enable the public body to identify a requested record (**section 14(1)(a)**); or
- a large number of records is requested or must be searched and responding within the time limit would unreasonably interfere with the operations of the public body (**section 14(1)(b)**).

**Model letters S, T and U** in Appendix 3 deal with the correction process. Guidance on making corrections and annotations, as well as copies of the **Request to Correct Personal Information Form** and the **Annotation to Personal Information Form** are included in Appendix 5.

### Transfer of requests for correction

**Section 37** provides authority for a public body to transfer a request for correction of personal information to another public body. This can occur when

- the other public body originally collected the personal information; or
- the other public body created the record containing the personal information.

This provision ensures that the public body that originally collected or compiled the information deals with a request for the correction of that personal information. It can also ensure that all public bodies to which the information was disclosed are properly notified of the correction. **Section 37** mirrors the provisions for transfer of access to information requests.

If a request is transferred under this section, the public body transferring the request must notify the individual of the transfer as soon as possible. The public body receiving the transferred request has 30 days from the date of the transfer to respond to the request, and can extend this time limit as outlined above.

## 7.5 Protection of Personal Information

**Section 38** of the Act requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

*Making reasonable security arrangements* means approving and implementing a security policy for use within a public body.

In *IPC Investigation Report F2003-IR-003*, the Investigator found that a school jurisdiction had failed to make reasonable security arrangements to protect personal information against unauthorized access. Most staff members had full access to the electronic Student Information Record System and the system had no way to track who was accessing student information, when, or for what purpose. The limited access controls that did exist had not been employed, and no policies, procedures or training were in place regarding access and privacy.

Government departments and offices must adhere to certain security policies produced by the Office of the Corporate Chief Information Officer, such as the *Government Security Policy for Disk Wiping Surplus Computers* and the *Policy for Maintaining the Security of Government Data Stored on Electronic Data Storage Devices*.

Other public bodies may store or dispose of personal information only as authorized by bylaw, resolution, or other legal instrument, or under the direction of the public body's governing body (**section 3(e)**).

Public bodies should document the transfer of records containing personal information to the Provincial Archives or other archives. Public bodies should also document the destruction of records containing personal information, except for transitory records.

Public bodies are responsible for ensuring that personal information is protected during the time it is in storage, waiting to be picked up, and in the process of being transferred to archives or destroyed.

Public bodies must ensure that contractors follow proper privacy protection procedures. When contracting for services involving personal information, public bodies should incorporate privacy protection provisions in the contract. For more information on contracting under the *FOIP Act*, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

For further information on

- conducting privacy compliance reviews and threat and risk assessments;
- reviewing forms and other collection instruments; and
- developing a security policy;

see Chapter 9.

---

**7.6**  
**Use of**  
**Personal**  
**Information**

**Section 39** of the Act lists the only circumstances under which a public body may use personal information. A public body may use personal information only

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose (**section 39(1)(a)**);
- if the individual the information is about has identified the information and consented, in the prescribed manner, to the use (**section 39(1)(b)**);
- for a purpose for which that information may be disclosed to that public body under **sections 40, 42 or 43 (section 39(1)(c))**; or
- if the information is in alumni records, for the purpose of a post-secondary educational body's own fund-raising activities (**section 39(2)**).

*Use of personal information* means employing it to accomplish the public body's purposes, for example, to administer a program or activity, to provide a service or to determine eligibility for a benefit. Public bodies may use personal information only under the following circumstances.

**For the original or a consistent purpose**

**Section 39(1)(a)** The *purpose* means the purpose for which the information was collected under **section 33**. A public body can use the information for that purpose. Typical purposes include the administration of a particular program, the delivery of a service and other directly related activities.

The purpose must conform to **section 33** of the Act, which limits the purposes for which information may be collected. The authority for collection of personal information (**section 33**) is discussed in section 7.1 of this chapter.

The purpose of collection is described in the collection statement provided to the individual when the information is collected directly. When the information is not collected directly, or when it is compiled from several sources, the purpose should be stated in the written policy or procedure dealing with the program.

*Compiled* refers to a process by which certain information is created and becomes tied to or associated with an identifiable individual. For example, a public body creates or assigns a student ID number for each student. This information becomes the personal information of the student but the information was compiled by the public body, not collected from the student (see *IPC Order 2001-038*).

A public body may make use of personal information it has gathered, created or manipulated for the specific purposes for which it is permitted to collect or compile it.

A *consistent purpose* is one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses the information (**section 41**).

**Section 39(1)(a)** also says that a public body may use personal information for a use that is consistent with the original purpose.

*Consistent use* is defined in **section 41** of the Act as a use that has a reasonable and direct connection to the original purpose of collection and that is necessary for performing the statutory duties of the public body.

In *IPC Order 2001-038*, the Information and Privacy Commissioner found that a school board's use and disclosure of a child's gender information for advertising, marketing and revenue generation purposes were not consistent with the original purpose for collection – namely, to register the child in school. However, use and disclosure of other personal information for the purpose of setting up and administering a student e-mail system was a consistent purpose.

Section 7.8 of this chapter deals more thoroughly with the concept of consistent uses.

For personal information held in personal information banks, public bodies must keep a record of all the purposes for which the personal information was collected or compiled and the purposes for which it is used or disclosed (**section 87.1(2)(d)**).

#### ***With the consent of the individual***

**Section 39(1)(b)** A public body may use personal information if the individual the information is about has identified the information and has consented, in the prescribed manner, to its use.

Consenting in the *prescribed manner* means that the public body has followed the procedures for obtaining consent set out in **section 7** of the FOIP Regulation. This states that consent

- must be in writing; and
- must specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.



To meet the minimum requirements under the Act, a form or other instrument requesting consent must

- specify to whom the personal information may be disclosed; and
- specify how the personal information may be used.



If consent is given in writing, the form must be signed by the person giving consent.

Consent may be given electronically or orally if the head of the public body has established a process for accepting electronic or oral consent that meets the requirements of section 7(5) or (6) of the Regulation, respectively.

Where appropriate, a form or other instrument requesting consent should

- indicate the original purpose of the collection, as well as the additional purpose for which the information is to be used and for which consent is being provided;
- indicate that consent is voluntary;
- indicate that consent may be revoked, but identify, where possible, any limitations and any consequences or implications that may result from revocation;
- to the extent possible, identify any consequences that may result from refusal to consent; and
- indicate the period of time during which the consent remains valid.

A public body may wish to seek consent for a new use of personal information. If the public body proposes to use personal information for a new purpose, the public body must get consent from the individual. If the public body is collecting additional information for a new use, the public body must have authority for the new collection and consent for the new use. The collection notice required under **section 34(2)** should be revised to indicate that the use of personal information collected from individuals after that time will be in accordance with the revised purpose.

It is important to note that, while a new use of personal information may be allowed under the Act with the consent of the individual, the public body may still be bound to adhere to its enabling enactments to authorize the new use. A public body cannot use personal information for programs that are outside the legislated area of responsibility of the public body. Also, if the public body is required to obtain additional personal information for the new use, then the collection of that personal information must be authorized by **section 33**.

Consent to a different use by the individual concerned serves as an indication that the person knows the consequences of the use of his or her personal information and has been provided with enough facts to make an informed decision about whether or not to consent to the use. When the person concerned has not indicated whether or not consent is given to a different use of personal information, public bodies cannot assume the individual has consented.



**The absence of consent for a new use of information previously collected must be interpreted as the absence of authorization to use the information for the new purpose, unless otherwise permitted under the Act.**

Public bodies cannot penalize individuals for refusing to give consent for use for an additional purpose by denying them any benefit or service provided in connection with the original collection. Individuals may, however, find they are denied a new benefit or service that might have been made available if the individual had consented to use of his or her personal information for that different purpose.

Section 2.5 of Chapter 2 deals with those classes of persons who may act for minors, incompetent persons, and other individuals in giving or withholding consent.

***For a purpose for which the information may be disclosed to a public body under section 40, 42 or 43***

**Section 39(1)(c)** This provision permits a public body to use personal information that has been disclosed to it by another public body under **section 40, 42 or 43** of the Act.

For example, the Students Finance Board may disclose a student's financial information to a housing management body in order to verify the amount of rent being paid by the student (**section 40(1)(l)**). The housing management body can use the financial information disclosed by the Students Finance Board in order to verify the rental amount. The housing management body cannot use the personal information for any other purpose unless that use for the other purpose is authorized under another provision of **section 39**.

**Section 39(1)(c)** also allows a public body to use personal information disclosed to it for research purposes by another public body under **section 42** or by the Provincial Archives or the archives of another public body under **section 43**.

***Information in alumni records of a post-secondary educational body for fund-raising***

**Section 39(2) and (3)** This provision states that a post-secondary institution may use personal information in its alumni records for the purpose of its own fund-raising. Post-secondary educational bodies should have procedures in place to inform new alumni of this use at the time of graduation. They should not rely on this provision, which was added to the Act in May 1999, to use the personal information of individuals who become alumni after 1999 for their fund-raising activities.

The use of this personal information is qualified by **section 39(3)**. This requires the public body to discontinue using an individual's personal information for fund-raising purposes when requested to do so by that individual.

Post-secondary educational bodies should take reasonable steps to inform their alumni of this provision, for example, placing a notice in a prominent place in the institution's alumni newsletter to give individuals a chance to request cessation of the activity, or providing alumni with an opportunity to request cessation of the activity when mailing lists are updated, or mailing a notice to all alumni. For more

information on this topic, see FOIP Bulletin No. 5: *Fund-Raising*, published by Access and Privacy, Service Alberta.

### **Limit on use of personal information**

**Section 39(4)** **Section 39(4)** sets some limits on the extent to which a public body can use the personal information in its custody or control.

A public body can use information only to the extent necessary to carry out its purpose in a reasonable manner. This limitation applies both to the amount and type of personal information being used.

This provision is intended to ensure that public bodies to which personal information is disclosed use the minimum amount of information necessary to achieve their purposes.

For example, employees in a particular program area who have access to personal information in an electronic database should be provided with access to only those data elements they require to do their job, not to the whole database. Employees could be given access to certain views or screens in a database, rather than access to the entire database.

It may be possible to anonymize data (e.g. by stripping identifiers) so that employees without access to the personal information can manipulate and analyze the data. Only a few authorized staff would have access to the individually identifying information that is initially collected, and a unique identification number could be assigned to the information or to the data subjects. The non-identifying data can then be used for various analytical or reporting purposes within the organization.

*In a reasonable manner* means in such a way that a public body is not required to implement overly restrictive procedures on the use of personal information when the information is not of a sensitive nature or when the use by others in the organization would not be an unreasonable invasion of personal privacy.

**Section 39(4)** mirrors the limitation provision with respect to the disclosure of personal information in **section 40(4)**.

---

#### **7.7 Disclosure of Personal Information**

**Section 40** of the Act lists the only circumstances under which public bodies may disclose personal information. **Section 40** provides for a response to an access request under **Part 1**, and for disclosure in the course of various administrative processes and in response to informal access requests.

Disclosure of personal information may occur *only* in the specific circumstances outlined in **section 40**. If **section 40** does not provide authority for a disclosure, the public body cannot disclose the information.

In *IPC Investigation Report 2001-IR-002*, the Investigator found that personal information about an investigation that was discussed at an *in camera* council meeting should not have been disclosed to a journalist since the disclosure was not authorized by any of the disclosure provisions of the Act.

**Section 40** does not authorize disclosure of personal information on the basis that a third party may obtain access to that information through other means (see *IPC Investigation Report F2002-IR-005*).

**Section 40** enables disclosure; it *does not require* disclosure. This is indicated by the word *may* in the introduction to the section. Public bodies should look at the circumstances surrounding each request and the privacy protection objectives of the Act when deciding whether to disclose personal information.

**Section 40(4)** states that a public body may disclose personal information only to the extent necessary to enable it to carry out the purposes described in **section 40(1), (2) and (3)**. These purposes are described in the following pages. Disclosure has to be carried out in a reasonable manner.

Public bodies should be careful to disclose only limited amounts of personal information.

For example, when a school division issued a letter to staff, students and parents regarding the death of a student, it should have simply notified them about the death and advised parents and staff of resources available to help the students. The school division should not have provided details about the death (see *IPC Investigation Report F2003-IR-002*). In *IPC Investigation Report F2004-IR-002*, a school district was found to have disclosed too much information when reports sent to parents about their children's alleged misbehaviour contained information about other students involved in separate incidents. (See also *IPC Order F2004-010*.)

Public bodies have a responsibility in most cases to clarify and understand the reasons for the request for disclosure. Disclosures should be made in a way that helps the requester and is cost-effective for the public body. This may mean that not all disclosures are in writing, or that, when a working relationship with another body has been established, all the proofs required are not asked for each time a request is made.

*Disclose* means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give personal information by any means to someone.

Although the Act applies to *recorded* information, **section 40** is not limited to the disclosure of *records*. Disclosure includes oral transmission of recorded information by telephone or in person; provision of personal information on paper, by facsimile copy or in another format; and electronic transmission through electronic mail, data transfer or the internet.

**Section 40** provides for disclosure

- to the person whose information it is, either in response to a routine request for information or in response to a request under **Part 1**;
- to an individual's personal representative who is entitled to exercise the rights of that individual under **section 84** of the Act;
- to any other person in response to an access request; as a disclosure in the public interest (**section 32**); when the disclosure would not be an unreasonable invasion

of privacy (**section 40(1)(b)**), or when **section 40** of the Act specifically allows the disclosure; or

- to other public bodies, to legislative, legal and judicial officers, to other levels of government, or to non-government organizations (in some cases the disclosure supports the activities of the public body disclosing the information; in other cases the disclosure supports the activities of the party receiving the information).

**Section 40** does not prevent the routine disclosure of an individual's personal information to that individual if the public body has adopted a policy of disclosing a particular category of personal information. In these circumstances, the public body will provide the personal information without a FOIP request.

Public bodies must keep a record of the purposes for which personal information held in any personal information banks may be disclosed (**section 87.1(2)(d)**) (see section 7.11 of this chapter).

Public bodies must also keep a record of any disclosures of personal information made under **section 40** for a purpose not included in the Directory of Personal Information Banks (**section 87.1(3)**). This may consist of a note on a file or a flag in an electronic system that refers to a paper record or another data file.



**A record of a disclosure is needed to enable a public body to comply with its obligation under section 36(4) to inform anyone to whom it has disclosed personal information, of any correction to that information.**

As a best practice, a record of a non-routine disclosure may include

- the name of the individual whose personal information is requested;
- the nature of the requested information and the purposes for which it will be used;
- the authority for the disclosure;
- the title, business address and business telephone number of the contact person in the requesting public body or agency; and
- the name and signature of the officer or employee of the public body who authorizes the use or disclosure.



**Public bodies must have appropriate administrative controls in place to ensure that personal information is disclosed only to authorized persons.**

When developing a new program, public bodies should consider whether personal information will need to be disclosed, and ensure the disclosure is authorized under the Act. Public bodies should also regularly review their disclosure policies and practices to ensure that they continue to meet the requirements of the Act. Where it is found that disclosures are not authorized, practices should be altered to meet legal requirements or discontinued. A review may be carried out in conjunction with a review of information practices and systems as discussed in Chapter 9.



Public bodies may disclose personal information only for the following purposes. Each permitted disclosure is outlined and discussed.

***Disclosure in accordance with Part 1 of the Act***

**Section 40(1)(a)** This provision permits disclosure to respond to access requests and to comply with the public interest disclosure provisions of the Act. Under this provision, a disclosure may take place when

- an applicant has requested access to his or her own personal information, subject to the exceptions in **sections 16 to 29** and to the paramouncy provision in **section 5**;
- an applicant has requested access to records containing personal information about another individual and disclosure of the personal information does not constitute an unreasonable invasion of the privacy of the other individual under **section 17**, subject to other exceptions and to third party notification requirements; or
- **section 32** applies.

***Disclosure that would not be an unreasonable invasion of a third party's privacy under section 17***

**Section 40(1)(b)** This provision permits disclosure in the clearest of cases after a complete analysis has been carried out under **section 17** and a determination made that the personal information would not be excepted under **section 17** in response to an access request. If there is any doubt as to whether the disclosure would be considered an unreasonable invasion of personal privacy, the public body should have the person who asked for the information submit an access request under **Part 1** of the Act.

When another provision of **section 40** permits disclosure, the disclosure should be made under the other specific provision. Examples are: disclosure with the consent of the individual, disclosure required or authorized by an Act of Alberta or Canada, and disclosure for research purposes.

**Section 40(1)(b)** gives public bodies flexibility in responding to requests for personal information that clearly would be provided if a FOIP request were made. It allows for a more helpful and timely response to such requests.

In some circumstances, public bodies will be able to establish policies and practices for routine disclosure in response to requests for particular classes of personal information (e.g. school transcripts). Policies and practices may also be established as a result of active dissemination of personal information without a request (e.g. publishing an employee directory). In establishing such policies, public bodies should determine whether any of the other exceptions outlined in **Part 1** of the Act might apply to the information (see section 2.4 of Chapter 2 for a discussion of providing routine access to records or information).

Examples of classes of personal information for which a policy might be appropriate include

- information about employee classification, salary range, employment responsibilities and discretionary benefits (**section 17(2)(e)**);

- financial and other details of a contract to supply goods or services (**section 17(2)(f)**);
- information regarding permits or licences relating to commercial or professional activities or real property (**section 17(2)(g)**);
- details of discretionary benefits of a financial nature (**section 17(2)(h)**); and
- personal information about an individual who has been dead for 25 years or more (**section 17(2)(i)**).

Public bodies may charge a fee for such information. For more information on **section 17(2)**, see section 4.3 of Chapter 4.

**Section 17(2)(j)** deals with a range of disclosures that can be made if disclosure is not contrary to the public interest. Individuals have the right to request that the information outlined in this provision not be disclosed. For this reason, requests for personal information that fall within the scope of **section 17(2)(j)** need to be considered on a case-by-case basis. A public body may take into consideration who is making the request, and why, in deciding whether to disclose the information.

If an individual has requested that the information not be disclosed, it cannot be disclosed under **section 40** unless another provision in that section permits the disclosure and the public body decides to disclose the information in accordance with that provision.

If disclosing the information could interfere with law enforcement or could reasonably be expected to affect someone's health or safety, the information should not be disclosed.

For more information on situations when disclosure might be made, see section 4.3 of Chapter 4 and FOIP Bulletin No. 4: *Disclosure of Personal Information "Not Contrary to the Public Interest"*, published by Access and Privacy, Service Alberta.

#### ***Disclosure for original or consistent purpose***

**Section 40(1)(c)** The *purpose* means the purpose for which personal information was collected under **section 33**. A public body can disclose personal information for that purpose. Typical purposes include the administration of a particular program, the delivery of a service and other directly related activities. Authority for collection is discussed in section 7.2 of this chapter.

Personal information is *compiled* when certain information is created and becomes tied to or is associated with an identifiable individual. For example, a public body creates or assigns a student ID number for each student. This information becomes the personal information of the student but the information was compiled by the public body, not collected from the student (see *IPC Order 2001-038*).

A *consistent purpose* is one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that discloses the information (**section 41**). A disclosure is therefore permissible if it is a logical extension of the original use.

Examples of disclosure for a consistent purpose include

- providing a list of participants in a program to another part of a public body for evaluation of the program; and
- disclosing the name and mailing address of the property owner for other purposes related to the operation of the municipality such as providing services and utilities.

A more detailed explanation of *consistent purpose* is provided in section 7.8 of this chapter.

### **Disclosure with consent**

**Section 40(1)(d)** This provision permits disclosure of an individual's personal information when the individual has identified the information and consented, in the manner prescribed in **section 7** of the FOIP Regulation, to the disclosure. This states that consent

- must be in writing; and
- must specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.

**To meet the minimum requirements under the Act, a form or other instrument requesting consent must**

- specify to whom the personal information may be disclosed; and
- specify how the personal information may be used.



**If consent is given in writing, the form must be signed by the person giving consent.**

**Consent may be given electronically or orally if the head of the public body has established a process for accepting electronic or oral consent that meets the requirements of section 7(5) or (6) of the Regulation, respectively.**

As a best practice and where appropriate, a form or other instrument requesting consent should

- indicate the original purpose of the collection, as well as the additional purpose for which the information is to be used and for which consent is being provided;
- indicate that consent is voluntary;
- indicate that consent may be revoked, but identify, where possible, any limitations and any consequences or implications that may result from revocation;
- to the extent possible, identify any consequences that may result from refusal to consent; and
- indicate the period of time during which the consent remains valid.

Examples of consent to disclosure include: consent to have references provided in support of job applications; consent to provide information to the Canada Revenue Agency in order to obtain income verification from that source; and consent to the use of photographs for promotional purposes.

*IPC Investigation Report 2000-IR-003* provides a discussion of the consent requirements under **section 40(1)(d)** and **section 7** of the FOIP Regulation. In that case, the Investigator found that an individual's consent to release information to a private landlord was not valid because the consent had been revoked prior to the time of disclosure.

When an individual copies ("cc"s) other parties on a letter or e-mail, this is not consent for the responder to disclose personal information to the parties who were copied (*IPC Orders F2002-018 and F2005-014*).

When the person concerned has not indicated any consent to disclose personal information, and no other provision exists to permit disclosure, public bodies cannot disclose the information.



**A public body must not penalize an individual for refusing to consent to a disclosure of personal information for a purpose other than the purpose for which the personal information was collected. A public body must not deny the individual the benefit or service for which the personal information was originally collected.**

A public body should not seek consent for a disclosure that is already authorized elsewhere in **section 40**, unless it intends not to disclose the personal information without the individual's consent.

Consent to a disclosure may be given by a representative acting on behalf of an individual in accordance with the conditions set out in **section 84(1)**. These conditions are discussed in detail in section 2.5 of Chapter 2.

Consent for a disclosure should be sought as early as possible after the need has been identified. Ideally, it should be sought at the time the information is collected. In such cases, the request for consent to disclose is added to the collection instrument. For more information on this topic, see FOIP Bulletin No. 17: *Consent and Authentication*, published by Access and Privacy, Service Alberta

***Disclosure to comply with an enactment of Alberta or Canada or with a treaty, arrangement or agreement under an enactment of Alberta or Canada***

**Section 40(1)(e)** This provision permits disclosure of personal information to comply with an Act of Alberta or Canada, a regulation made under such an Act, or with a treaty, arrangement or agreement made under either an Act or a regulation. It does not apply to the legislation of other provinces, territories or foreign states.

Disclosure to *comply with an enactment of Alberta or Canada* means disclosure of personal information as *required* by either provincial or federal legislation. There

must be a direct relationship between complying with the enactment and the disclosure of the personal information.

Disclosure to *comply with a treaty, arrangement, or agreement* made under an enactment of Alberta or Canada means disclosure of personal information as *required* by the treaty, arrangement or agreement. The enactment must provide authority for the provision in the treaty, arrangement or agreement, and that provision must specifically authorize disclosure of the personal information.

A *treaty* is a formally concluded and ratified agreement between or among independent states. Only the federal government of Canada has the power to conclude treaties with foreign countries. An example of a treaty permitting the exchange of personal information is the *Mutual Legal Assistance Treaty*, which provides for the exchange of information on a variety of law enforcement matters.

An *arrangement* is a coming to terms on how certain matters will be conducted, particularly if there is no formal agreement documenting this. Often administrative arrangements are managed without an agreement but there must still be authority under an enactment for entering into the arrangement, for the purposes of **section 40(1)(e)**. Arrangements should, whenever possible, be in writing. A verbal arrangement should be allowed only in very exceptional circumstances, such as sensitive law enforcement, security or intelligence matters, and only at the insistence of one or more of the parties. Where an arrangement is unwritten, disclosures should be approved at a senior level within the public body.

An *agreement* documents the obligations and responsibilities of the parties and what actions are to be taken. For the purposes of **section 40(1)(e)**, authority for the agreement or for entering into the agreement must be contained in an enactment of Alberta or Canada. *Agreements* include contracts, memoranda of understanding, collective agreements, etc. All agreements should be in writing.

Agreements concerning the disclosure of personal information by public bodies to other organizations, including federal, provincial, municipal, and foreign governments, as well as international bodies, should contain

- a description of the personal information to be collected or disclosed;
- the authority for collecting, using and/or disclosing personal information;
- the purposes for which the information is to be collected, used or disclosed, including a restriction on subsequent uses;
- a statement of all the administrative, technical and physical safeguards required to protect the confidentiality of the information, especially with respect to its use and disclosure;
- a statement specifying whether information received by a public body will be subject to the provisions of the *FOIP Act* or, for other jurisdictions where comparable legislation exists, whether that legislation will apply;
- a statement that the disclosure of the personal information will cease if the recipient is discovered to be improperly disclosing the information collected from the public body; and



- the names, titles and signatures of the officials in both the supplying and receiving public bodies who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.

Examples of such agreements include agreements for

- the exchange of personal information about individuals who have applied for social assistance from the Province with Human Resources and Social Development Canada to determine whether they are also receiving employment insurance;
- the exchange of personal information about applicants for the Alberta Seniors Benefit with Alberta Health and Wellness so that applicants can obtain seniors' health benefits; and
- the disclosure of personal information by schools to health authorities for the purpose of immunization and other preventive health services.

Public bodies should maintain a list of all agreements, arrangements and treaties, as applicable, under which they disclose personal information. Public bodies should include information disclosed under agreements, arrangements and treaties in the relevant personal information bank descriptions contained in the directory of personal information banks which the Act requires to be published by the public body (**section 87.1(2)(d)**).

For further information, see section 9.7 of Chapter 9 and *Guide to Developing Personal Information Sharing Agreements*, published by Access and Privacy, Service Alberta.

FOIP Bulletin No.15: *Disclosure of Personal Information to Unions: Before a First Agreement*, published by Access and Privacy, Service Alberta, discusses whether the personal information of employees may be disclosed to a union before a collective agreement is in place. It also discusses the more general issue of applying the *FOIP Act* to the disclosure of employee personal information to unions under a collective agreement.

***Disclosure that is authorized or required by an enactment of Alberta or Canada***

**Section 40(1)(f)** This provision is related to **section 40(1)(e)**. However, whereas in **section 40(1)(e)** disclosure must be *for the purpose of complying* with an enactment, and is therefore likely to be required by law, in **section 40(1)(f)** disclosure is permitted if it is either required or *authorized* by an enactment of Alberta or Canada. If disclosure of personal information is authorized – but not required – by an enactment, the head of the public body has more discretion as to whether or not to disclose the information.

Examples of Acts that *require* disclosure of personal information include the *Legislative Assembly Act*, the *Public Lands Act*, the *Public Trustee Act* and the *Maintenance Enforcement Act*.

Some Acts require a particular public body to disclose personal information for the purpose of the (disclosing) public body's program. For example, section 50 of the *Public Lands Act* requires the Minister responsible for that Act to disclose certain personal information to the public as part of the enforcement process.

If a public body is relying upon **section 40(1)(f)** as authority to disclose personal information, it must ensure that the disclosure is strictly in compliance with the enactment that authorizes the disclosure. For example, in *IPC Investigation Report 99-IR-008*, the Information and Privacy Commissioner's investigator found that the disclosure contravened the *Workers' Compensation Act* because it was a disclosure of information that was not relevant to the administration of the *Workers' Compensation Act* or its regulations.

Some Acts require *other* bodies to disclose personal information to a particular public body for the purposes of the (collecting) public body's program. For example, under the *Public Trustee Act*, section 44, the Public Trustee may compel a public body that has possession of personal, financial or health-related information about a client or potential client to provide that information or record to the Public Trustee to carry out a task, duty or function relating directly to the client or potential client.

Sections 12 and 13 of the *Maintenance Enforcement Act* require a list of personal information (e.g. financial information, an identification number issued by a province) to be disclosed to the Director of Maintenance Enforcement by government departments, provincial agencies (e.g. post-secondary institutions) as well as business organizations (including municipalities). Only the requested information that is listed in that Act should be disclosed by a public body and collected by the Director.

Examples of Acts that *authorize* disclosure of personal information include the *Charitable Fund-raising Act*, the *Workers' Compensation Act* and the *Dependent Adults Act*.

Before disclosing personal information under **section 40(1)(f)** in response to a request, a public body should ask the body requesting the information to provide their legal authority for collecting the information. A public body requesting personal information from another body should provide the disclosing body with their legal authority for collecting the information.

#### ***Disclosure to comply with a subpoena, warrant or order***

**Section 40(1)(g)** This provision permits personal information to be disclosed in order to comply with legal processes that require the production of information. These processes include the use of a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information, or with a rule of court binding in Alberta that relates to the production of information.

A *subpoena*, also called a "summons to witness," is a command issued by a party in litigation requiring the attendance of someone as a witness at a court proceeding or hearing. It will specify a certain place and time when testimony on a certain matter will be required, and may also order a person to meet the requirements of a court to disclose information.

Time is usually of the essence in dealing with a subpoena, as it is often served with very little notice. Public bodies cannot ignore subpoenas since they would risk being cited for contempt of court and, at a minimum, fined.

A *warrant* is a judicial authorization to collect information – in this context, personal information.

An *order* is an authoritative command, direction or instruction to produce something – again in this context, personal information.

The court or tribunal must have jurisdiction in Alberta to require a public body to disclose information. Courts with jurisdiction in Alberta include the Supreme Court of Canada, the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, the Provincial Court of Alberta, as well as the Federal Courts.

Where a tribunal has the power to compel the production of information under legislation of Alberta or Canada, that tribunal has jurisdiction in Alberta. An example of a federal tribunal with jurisdiction in Alberta is the Canadian Radio-Television and Telecommunications Commission.

A court or tribunal of another country or of a province or territory of Canada other than Alberta does not have jurisdiction in Alberta. However, an order of such a court or tribunal may be enforceable in Alberta under legislation of Alberta that provides for the reciprocal enforcement of orders, or a court procedure that makes an order filed with a court in Alberta enforceable as an order of the Alberta court (e.g. Alberta's *Interprovincial Subpoena Act*).

The *FOIP Act* also establishes offences and penalties for disclosure in response to a subpoena, warrant or order if the disclosure is not permitted under **section 40(1)(g)**, and no other provision of the *FOIP Act* permits disclosure. For further information on offences under the *FOIP Act*, see section 2.11 of Chapter 2.

Although **section 40(1)(g)** enables, but does not require disclosure, public bodies normally comply with orders, warrants or subpoenas because they have the force of law. However, a public body should not automatically assume that an order, warrant or subpoena is valid in Alberta.



**Public bodies should consult their legal advisor when they receive a court order, warrant or subpoena in order to determine whether it refers to information that is actually in the custody or under the control of the public body, whether the instrument has been served properly, whether the court has jurisdiction in Alberta and whether there is some compelling reason to oppose the order, warrant or subpoena. They will also need to ensure that the amount and type of information disclosed is actually required by the instrument.**

***Disclosure to an officer or employee of the public body, or to a member of Executive Council***

**Section 40(1)(h)** This provision permits disclosure of personal information to officers or employees of the public body that has custody or control of the personal information, and to Cabinet members. It does not allow disclosure to employees or officers of other public bodies.

An *employee* is defined in **section 1(e)** of the Act to include a person retained under contract to perform services for the public body, a volunteer and an appointee to a board or committee.

Members of a school council are not employees of a school board for the purposes of the *FOIP Act* (*IPC Order 2001-010*) but school volunteers are employees (*IPC Investigation Reports 98-IR-015 and 2001-IR-005*).

The term *officer* is included to ensure that all persons working for a public body in any capacity are encompassed by the provision. This includes an elected official, such as a school board trustee, when the official is acting on behalf of the public body to carry out the mandate and functions of the public body, as opposed to functioning as a representative of his or her constituents (see *IPC Order 99-032*).

A *member of the Executive Council* includes the President of Executive Council, a Minister, and an Associate Minister (described in the *Legislative Assembly Act* as a "Minister without Portfolio").

**Section 40(1)(h)** does not allow an official or employee or member of the Executive Council to have automatic access to all personal information within a public body.



**The test for disclosure is whether the information is necessary for the performance of duties. Disclosure is permissible only if access to the particular personal information is needed to do a job or deal with a particular situation.**

The persons to whom the information is disclosed should be able to prove a need to see, or handle the personal information in order to do their jobs. The following are some examples of cases where disclosure might be necessary for the performance of an employee's duties.

- Human Resources may require access to the résumés of applicants in order to carry out the recruitment function.
- Where there is a formal process within a public body to do so, an employee may need to report a suspected fraud (e.g. an alleged contravention of the Government of Alberta's Code of Conduct and Ethics).
- Service counter staff may need to be informed if a client has a history of acting violently when interacting with departmental staff and if there is a need for extra security when the individual approaches the office.
- A counsellor may require access to student records to provide assistance, at the request of a teacher, to a student who is not doing well in school.
- The head of a local public body may require information to prepare a report for the governing body.
- A Minister may need background information about an issue and the people he or she is meeting with in order to understand the problem and their needs.

An example of a permitted disclosure under **section 40(1)(h)** was the disclosure of the nature of a complaint against an employee under **section 40(1)(h)** to another staff

member, since the information was necessary for that staff member to fulfil his duties of assigning employees to working groups (*IPC Investigation Report 99-IR-005*).

In another example of permitted disclosure, a school board disclosed a letter responding to a complaint to its Superintendent. The Superintendent was an officer or employee of the school jurisdiction and one of his duties was to review complaints made about the jurisdiction. Without knowledge of the personal information in the matter, the Superintendent could not properly perform his duty (*IPC Order F2002-018*).

***Disclosure for a common or integrated program or service***

**Section 40(1)(i)** This provision is similar to **section 40(1)(h)**, but permits disclosure to officers or employees of *another* public body when two or more public bodies are working together to provide or deliver a common or integrated program or service. The disclosure must be necessary for the delivery of the program or service *and* for the performance of the duties of the receiving employee, official, or member of Executive Council. **Section 40(1)(h)** does not allow disclosure to an organization that is not a public body (e.g. for a program offered in partnership with a private contractor).

A *common or integrated* program or service means a single program or service that is provided or delivered by two or more public bodies; or a program or service that has several distinct components, each of which may be provided or delivered by a separate public body, but which together constitute the program or service.

Each public body partner must be integral to the program or service. For example, a nursing practicum program requires the participation of both the post-secondary institution, and the health care body; the program would not function without the services of each body. In contrast, an arrangement where several public bodies contract with the same information technology service provider is *not* a common or integrated program or service.

**Section 40(1)(i)** allows for the sharing of personal information between the public bodies in order to deliver the service to the clients. A common client does not, of itself, meet this definition. Factors that will determine whether or not a program or service meets the definition include

- evidence of joint planning;
- a formal agreement or legislative authority for working together;
- common goals expressed by the partners; and
- evidence of collaboration or cooperation in delivery.

When public bodies are implementing such programs or services, they should

- disclose information in non-identifiable form whenever possible;
- ensure that individuals participating in the program are notified of all the partners and of the sharing of personal information;
- disclose personal information only to those who need to know about a particular individual;



- disclose personal information only to the extent necessary for program or service delivery; and
- ensure that personal information is not used for any other purpose.

Examples of such programs and services include

- children's service initiatives delivered through Child and Family Service Authorities;
- conjoint nursing programs that require the disclosure of personal information between program departments of different post-secondary institutions;
- work placement and practicum programs;
- school-housed public libraries; and
- centralized human resource programs.

For further information, see FOIP Bulletin No. 8: *Common or Integrated Programs or Services*, published by Access and Privacy, Service Alberta.

***Disclosure to enforce a legal right of the Government of Alberta or a public body***

**Section 40(1)(j)** This provision permits the disclosure of personal information to enforce a legal right that the Government of Alberta or a public body has against any person.

The Information and Privacy Commissioner considered criteria for applying this provision in *IPC Order F2005-002*. In that Order the Appeals Commission for Workers' Compensation owed a common law duty of fairness to the parties appearing before it. The Workers' Compensation Board was enforcing its legal right to a fair hearing when it disclosed personal information about a member of the Commission in a complaint alleging bias on the part of the member.

In most cases, the disclosure of personal information under this provision will be to the legal representatives of the public body or, in the case of public bodies such as government departments, to Alberta Justice and the Minister of Justice and Attorney General as the provincial government's legal representative. The legal rights may relate to civil or criminal law.

***Disclosure to collect a fine or debt or to make a payment***

**Section 40(1)(k)** This provision permits disclosure of personal information to

- collect a fine or debt owing to the Government of Alberta or a public body or an assignee of either of them; or
- make a payment owed by the Government of Alberta or a public body.

A *fine* is a monetary punishment imposed on a person who has committed an offence, including an offence under a bylaw.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

An *assignee* is the person who has been given, or assigned, the right to receive and enforce the fine or debt.

Documentation for the disclosure under this provision should be in writing and specify

- the nature of the information to be disclosed;
- the name of the public body, person or organization receiving the information;
- any other necessary identifying information, such as a case or file number;
- the purpose of the request, including a citation of the legal authority for collecting the fine or debt; and
- the name, title and business address of the official making the decision to disclose.

The provision permits disclosure to Crown Debt Collections of Alberta Finance and Enterprise or to a private collection agency to which the debt has been assigned. It does not permit disclosure to assist a collection agency, or any other person or organization that is not a public body, to collect a debt owed to another public body, or to person or organization that is not a public body.

This provision enables public bodies to disclose personal information for the collection of a fine or debt owed to the Government of Alberta or a public body, or to make a payment owed by the Government of Alberta or a public body. Many public bodies have authority to collect fines and debts in their legislation, and some legislation also authorizes a public body to disclose personal information to another public body for the collecting body's purposes. This provision is intended to assist public bodies in cases where their legislative mandate does not specifically extend to the disclosure of personal information for the purposes of collecting fines and debts. **Section 40(1)(k)** gives them an authority to pursue these activities.

**Section 40(1)(k)** does not permit information to be disclosed by a public body for the purpose of determining whether a fine, debt or a benefit is owed. This decision must be made before the information is disclosed.

The information disclosed should be the minimum needed to collect the debt. Usually this will be the name, last known address and telephone number, and any contact information provided by the individual. It is generally not necessary to disclose the reason for the fine or debt (e.g. a penalty imposed as a result of an offence under an Act).



**Disclosure of personal information under section 40(1)(k) should always be in writing.**

The provision also authorizes public bodies to disclose personal information for the purpose of making a payment owing by the Government of Alberta or by a public body to an individual (**section 40(1)(k)(ii)**). For example, the name of the individual, the amount of the payment to be made and the transaction number would need to be disclosed to Alberta Finance and Enterprise or to its agent, Payment Systems Corporation, in order to generate the cheque for the payment.

**Disclosure to determine or verify suitability or eligibility for a program or benefit**

**Section 40(1)(l)** This provision permits the disclosure of personal information to determine an individual's suitability or eligibility for a program or benefit, or to verify continuing eligibility for the program or benefit.

**Section 40(1)(l)** allows personal information to be disclosed when there is a need to determine whether or not an individual meets the eligibility or suitability criteria for a particular program or benefit. A public body may disclose personal information to another public body, or to an organization or institution, to allow the disclosing public body to determine or verify suitability or eligibility.



**Normally, disclosure will only be made after an individual has applied to participate in a program or for a benefit. Public bodies collecting this information should comply with the guidelines set out in sections 7.1, 7.2 and 7.3 of this chapter.**

*Eligibility* means whether a person qualifies for a program or benefit.

*Suitability* means the characteristics of an individual that enable him or her to be chosen for a program or benefit.

Examples of disclosures that might be permitted under this provision include

- verification of employment information when someone applies for employment insurance or employment counselling;
- disclosure of information from a seniors' lodge to a health authority to determine suitability for nursing home care;
- confirmation of membership in a library when an individual uses his or her library card in another library; and
- disclosure of information about attendance or marks to enable a second year of grant support to a student.

**Disclosure for audit purposes**

**Section 40(1)(m)** This provision permits the disclosure of personal information for audit purposes to the Auditor General (Alberta) and to other persons and bodies specified in the FOIP Regulation.

The *Auditor General* is an Officer of the Legislature appointed by the Lieutenant Governor in Council. The role of the Auditor General is to examine the accounts and records of the government relating to the consolidated revenue fund and all public money, including trust and special funds under the management of the government relating to public property. The Auditor General must report annually to the Legislature on his or her work, including findings as to whether or not departments and other public bodies have carried out their financial responsibilities. This provision does not apply to the Auditor General of Canada.

*For audit purposes* means for the purposes of carrying out a financial or other formal and systematic examination or review of a program, portion of a program or activity that includes personal information about individuals, provided such examination or review is sanctioned by statute, regulation or public policy relating to the public body (**section 8** of the FOIP Regulation). In the case of a local public body, the audit may be sanctioned by bylaw or resolution. Audit purposes do not include operational or administrative purposes such as verification of a claimant's eligibility for a program, benefit or service, where a decision would be made about a specific individual.

The persons to whom personal information may be disclosed for audit purposes are also specified in **section 8** of the FOIP Regulation. Disclosure may be made to persons who are employees of a public body, including a person retained under contract to perform services for the public body for audit purposes (as defined above).

When a contractor is hired to conduct an audit requiring disclosure of personal information under this provision, the contractor should be advised of, and agree to abide by, the provisions of the *FOIP Act*, as well as policy relating to the protection of privacy under the *FOIP Act*. For further information on contracting under the *FOIP Act*, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

Examples of disclosures that may be permitted under this provision include:

- disclosure to the Office of the Chief Internal Auditor of the Government of Alberta, and internal auditors of a municipality;
- disclosure to an accounting or audit firm engaged to conduct a financial audit of a public body;
- disclosure to a person auditing methods a housing management body uses to determine eligibility for low income housing; and
- disclosure for personnel audits, such as classification reviews or quality assurance audits of the work being performed.

***Disclosure to a Member of the Legislative Assembly***

**Section 40(1)(n)** This provision permits disclosure of an individual's personal information to a Member of the Legislative Assembly if the individual has requested assistance from the Member in resolving a problem.

A *Member of the Legislative Assembly (MLA)* is a person elected as a representative of a constituency within the province of Alberta to represent the interests of the voters in that constituency in the Legislative Assembly.

This provision permits disclosure only to Members of the Legislative Assembly of Alberta, and only to assist the person concerned to resolve a problem.

The provision *does not* permit the disclosure of personal information to federal Members of Parliament or municipal representatives. These representatives may, however, obtain personal information about an individual with his or her consent.

The purpose of disclosure under **section 40(1)(n)** must be to *assist in resolving a problem*. This includes helping an individual to provide information to a public body, inquiring about decisions or about a service or benefit, or correcting a mistake or misunderstanding. Where resolution of the problem is relatively straightforward, the public body can discuss the issue with the MLA and, with his or her agreement, simply call the individual concerned and provide the information directly.

The written consent of the individual concerned is not normally necessary for disclosure to MLAs under this provision. If possible, the enquiry and disclosure should be recorded in writing. Where enquiries and disclosures take place orally, the transactions should be noted on the person's file.

In cases where the information is particularly sensitive (e.g. medical, financial or law enforcement information), the public body may wish to obtain the written consent of the individual concerned before disclosing the information.



**Public bodies should have a policy in place for disclosure of personal information and should inform MLAs of their policy if a request is received for information.**

It is likely that the MLA will pass the personal information he or she receives from a public body to the individual concerned. Under this provision, public bodies can only disclose evidence of the request for assistance and personal information about the individual requesting assistance. Public bodies should also be cautious not to disclose personal information about third parties, such as the individual's family members under this provision.

#### ***Disclosure to a representative of a bargaining agent***

**Section 40(1)(o)** This provision permits disclosure of personal information to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an enquiry.

*Bargaining agent* refers to a union or other organization that negotiates on behalf of workers with their employers for improvements in pay, hours, benefits, and other working conditions, and that works to protect the rights of employees.

The individual must sign and date a statement of authorization or representation clearly stating to whom the information may be disclosed and for what purpose. Disclosure is limited to personal information that is necessary for the purpose of making an enquiry. The representative may receive only that personal information that the employee has specifically authorized for release.

The representative, unless duly authorized as the employee's representative, may not exercise the employee's right of access to the rest of his or her personal information. Nor can he or she exercise the right to request correction of the employee's personal information.

Public bodies should ensure that their employees understand the purposes of the Act with respect to protection of personal information and the way the Act is applied in circumstances where a bargaining agent requests information about an employee.



See also the discussion of **section 40(1)(e)** above for disclosure for the purpose of complying with a collective agreement made under an enactment of Alberta or Canada.

***Disclosure for archival purposes***

**Section 40(1)(p)** This provision permits disclosure of personal information to the Provincial Archives of Alberta or the archives of a public body for permanent preservation.

The *archives of a public body* means

- a public body's own archives, in which case the records will remain in the custody or under the control of that public body (e.g. the archives of most post-secondary institutions);
- the archives of another public body, to which records are transferred as authorized under **section 3(e)**, in which case custody and control of the records will normally be transferred to the archives; or
- an archival facility that operates under a contract or agency relationship with the public body (e.g. the Glenbow-Alberta Institute), in which case custody may be transferred but control must be retained by the public body.

This provision does not permit disclosure to private archives such as those run by a private museum or historical society.

**Section 40(1)(p)** permits the disclosure of personal information to the personnel of the archives to obtain an archival appraisal to determine what personal information may have long-term archival and historical value.

This provision also permits the transfer and deposit of the records in the Provincial Archives or the archives of a public body, for ongoing research purposes.

Disclosure by the archives is governed by **section 43** of the Act (see section 7.10 of this chapter).

***Disclosure to assist law enforcement***

**Section 40(1)(q)** This provision permits the disclosure of personal information to a public body or a law enforcement agency in Canada to assist in an investigation

- undertaken with a view to a law enforcement proceeding; or
- from which a law enforcement proceeding is likely to result.

*Law enforcement* is defined in **section 1(h)** of the Act and further explained in section 4.6 of Chapter 4.

A *law enforcement agency in Canada* includes a variety of agencies that are responsible for enforcing statutes. Examples of law enforcement agencies that are public bodies are Alberta Solicitor General (*IPC Order 96-007*), provincial and municipal police services, the Alberta Fire Commissioner's Office and provincial and municipal conservation services. The RCMP and First Nations' police services, Canada Revenue Agency and the Federal Superintendent of Financial Institutions are law enforcement agencies in Canada that are not public bodies.

*Proceeding* means an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions.

A *law enforcement proceeding* is a proceeding that leads or could lead to a penalty or sanction under a statute or regulation. Law enforcement proceedings include not only formal court proceedings but also proceedings of administrative tribunals, such as the Alberta Labour Relations Board. The penalty or sanction can be imposed by the public body conducting the proceeding (e.g. the Environmental Appeals Board) or by another body (e.g. a court).

When disclosing personal information under **section 40(1)(q)**, the public body should satisfy itself that

- the requesting party is a public body within the meaning of **section 1(p)** or is a law enforcement agency;
- there is a law enforcement investigation and that the investigation has been undertaken in contemplation of a law enforcement proceeding as defined in **section 1(h)** (i.e. a proceeding that can result in a penalty or sanction under a statute or regulation); and
- the requesting public body or law enforcement agency can provide the legal authority for the law enforcement activity.

Under **section 40(1)(q)(ii)**, the disclosure of personal information must be to assist an investigation from which a *law enforcement proceeding is likely to result*. When disclosure is contemplated before an actual law enforcement proceeding is under way, it must be probable that a law enforcement proceeding will go forward.

Public bodies that are also custodians under the *Health Information Act* must follow the rules in that Act regarding the disclosure of individually identifying health information to a law enforcement agency.



**A request by a law enforcement agency for personal information should be in writing and should be retained by the public body in support of any subsequent disclosure of personal information to that agency.**

A model **Law Enforcement Disclosure Form** is provided in Appendix 5. Law enforcement agencies are encouraged to use this or a similar form when requesting disclosure of personal information.

Public bodies should ensure that requests for personal information from law enforcement agencies are justified and contain

- the name of the individual whose information is requested;
- the exact nature of the information desired;
- the authority for the investigation;
- the purpose for which the requesting agency will use the information; and
- the name, title and address of the person authorized to make the request.

The record of disclosure should normally be kept in a separate file that documents all requests for disclosure from law enforcement agencies, since this record may itself qualify for an exception under **section 20** of the Act.

For further information on the meaning of law enforcement, see FOIP Bulletin No. 7: *Law Enforcement*, published by Access and Privacy, Service Alberta.

**Disclosure among law enforcement agencies**

**Section 40(1)(r)** This provision permits a public body that is a law enforcement agency to disclose personal information

- to another law enforcement agency in Canada; or
- to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

This provision permits law enforcement agencies in Alberta to exchange personal information with their federal, provincial and municipal counterparts in Canada. Examples include the RCMP, provincial securities commissions and other police services.

As well, the provision permits disclosure to law enforcement agencies in foreign countries. This includes police forces and other law enforcement organizations in other countries, international law enforcement organizations and municipal and state police forces in foreign countries. Examples would be the Metropolitan Police in England, the Federal Bureau of Investigation and the United States Citizenship and Immigration Services, and Interpol.

Disclosures under **section 40(1)(r)(ii)** must be made in accordance with an arrangement, written agreement, treaty or legislative authority. The same conditions for an arrangement, agreement or treaty apply as for **section 40(1)(e)** described above.

*Legislative authority* means a statute, regulation or other legislative instrument.

**Disclosure in case of injury, illness or death**

**Section 40(1)(s)** This provision permits disclosure of personal information so that a spouse or adult interdependent partner, relative or friend of an injured, ill, or deceased individual may be contacted. For the meaning of these terms, see the discussion of **section 40(1)(cc)** below.

**Section 40(1)(s)** also allows disclosure of personal information such as whether the individual has been taken to a hospital or requires assistance to get home.

**Disclosure in accordance with section 42 or 43**

**Section 40(1)(t)** This provision permits the disclosure of personal information for research and statistical purposes. The conditions applicable to research disclosures are discussed in sections 7.9 and 7.10 of this chapter.

**Disclosure to an expert for the purposes of section 18(2)**

**Section 40(1)(u)** This provision allows a public body to fulfil its obligations under **section 18(2)** of the Act. It allows the expert to determine whether or not release of the applicant's own information to the applicant could reasonably be expected to result in immediate and grave harm to the applicant's health or safety.

**Section 6** of the FOIP Regulation establishes conditions for the disclosure of personal information to a chartered psychologist or other appropriate expert as follows:

- the public body may disclose information relating to the mental or physical health of an individual to an expert for an opinion on whether disclosure of this information could reasonably be expected to result in immediate and grave harm to the individual's safety or mental or physical health;
- an expert to whom information is disclosed must not use the information except for the purposes of determining the harm described above;
- the public body must require an expert to whom the information will be disclosed to enter into an agreement relating to the confidentiality of the information; and
- if a copy of the record containing information relating to the mental or physical health of an individual is given to an expert for examination, the expert must, after giving the opinion, return the copy of the record to the public body or dispose of it in accordance with the agreement between the public body and the expert.

**Disclosure for use in a court or quasi-judicial proceeding**

**Section 40(1)(v)** This provision permits disclosure of personal information for use in a proceeding before a court or quasi-judicial body to which the Government of Alberta or a public body is a party.

A *quasi-judicial body* refers to a body whose members have a duty to hold a hearing; their decision affects the rights of the applicant; they use an adversarial process or proceeding to decide the issue before them; and they have an obligation to apply substantive rules (see *IPC Order 99-025*). A quasi-judicial body exercises judicial functions that are similar to that of a court or a judge. Examples of quasi-judicial bodies are the Alberta Labour Relations Board and the Alberta Transportation Safety Board. For more information about quasi-judicial bodies see section 1.5 in Chapter 1.

**Section 40(1)(v)** permits the disclosure of personal information to the legal representatives of the Government of Alberta or a public body for use in these proceedings. It also permits disclosure to the members of the quasi-judicial body or court.

Disclosure is normally to, or through, the legal representative of the public body or, in the case of public bodies that are government departments, Alberta Justice and Attorney General, which represents the provincial government in legal matters. Information may be disclosed to the legal representative of the other parties to a proceeding in accordance with the court disclosure and discovery rules that apply.

In cases where the Government of Alberta or the public body is not a party to the proceeding, **section 40(1)(f)** (disclosure in accordance with an enactment of Alberta

or Canada) may authorize or require disclosure. Examples of enactments that may authorize or require disclosure of personal information for use in a court or quasi-judicial proceeding include the Alberta Rules of Court (as interpreted by the courts), statutes governing the proceedings of administrative tribunals and statutes governing the disciplinary proceedings of professional regulatory organizations. See the discussion of **section 40(1)(f)** above.

***Disclosure to a place of lawful detention***

**Section 40(1)(w)** This provision permits the Minister of Justice and Attorney General or an agent or lawyer of the Minister to disclose personal information to a place of lawful detention in order to provide for the appropriate supervision of any individual detained in custody.

***Disclosure for the management or administration of personnel***

**Section 40(1)(x)** This provision allows a government department to disclose personal information about an employee or prospective employee, such as reference information, to another government department for the purpose of managing or administering personnel. The provision recognizes the provincial government as one employer for all provincial government departments.

**Section 40(1)(x)** also allows other types of public bodies to disclose the same kind of information *within* their own public body for the purpose of managing or administering their own personnel.



**No disclosure of personal information is permitted to other public bodies or to the private sector without the written consent of the individual, unless the disclosure is authorized under another provision in section 40.**

For example, if an employee of one school board asks for a reference about a prospective employee from the prospective employee's supervisor in another school board or in a post-secondary educational institution, disclosure of the reference information would require the prospective employee's consent.

*Management of personnel* refers to aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees (*IPC Investigation Report 2001-IR-006*). This includes staffing requirements, job classification or compensation, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training and development, occupational health and safety, and separation and layoff. For the Government of Alberta, the term includes the government-wide network managed through Corporate Human Resources. It does not, however, include the management of contracts for consultants, professionals or independent contractors.

**Section 40(1)(x)** does not permit disclosure of employment-related personal information to a prospective outsource operator during negotiations for privatization without the employees' consent. In *IPC Investigation Report 2001-IR-006*, the Investigator found that such a disclosure was not made for the purpose of managing the public body's personnel and was therefore not authorized by **section 40(1)(x)**.



*Administration of personnel* comprises all aspects of a public body's internal management, other than management of personnel, necessary to support the delivery of programs and services. Administration includes business planning, financial, materiel, contracts, property, information and risk management (*IPC Investigation Report 2001-IR-006*).

Employees should be informed, in a general way, of how they should expect their personal information to be collected, used and disclosed within the personnel management system. Disclosure of personal information for the purposes of the management or administration of consultant, or professional or other personal service contracts should be addressed in the terms of the contracts.



**Disclosures under section 40(1)(x) are permitted only within the official framework that governs the management and administration of personnel within a public body or across the Government of Alberta.**

Disclosure of personnel information is discussed in more detail in the publication produced for local public bodies by Access and Privacy, Service Alberta, entitled *Human Resources Guide for Local Public Bodies*.

#### ***Disclosure to enforce maintenance orders***

**Section 40(1)(y)** This provision permits the disclosure of personal information about individuals to the Director of Maintenance Enforcement for the purposes of enforcing a maintenance order under the *Maintenance Enforcement Act*.

The information disclosed may be about an individual who is the subject of a maintenance order or an individual who is the beneficiary of a maintenance order. For example, the Director of Maintenance Enforcement may require information about the current registration of a student at a post-secondary institution in order to determine whether a parent is required to continue to provide financial support for that individual.

Sections 12 and 13 of the *Maintenance Enforcement Act* require the list of personal information (e.g. financial information, an identification number issued by a province) to be disclosed to the Director of Maintenance Enforcement by government departments, provincial agencies (e.g. post-secondary institutions) as well as business organizations (including municipalities). Only the requested information that is listed in that Act should be disclosed by a public body and collected by the Director.

The provisions also require provincial agencies to withhold support payments (e.g. student loan funds) to beneficiaries of provincial programs who have defaulted on maintenance support payments for a specified period of time. The provincial agency may be required to provide information about the beneficiary before paying out the funds.

Under this provision, a public body can only disclose personal information to the Director of Maintenance Enforcement or someone delegated to act on his or her behalf. A public body should require that the request be made in writing.

**Disclosure to an officer of the Legislature**

**Section 40(1)(z)** This provision permits the disclosure of personal information to an officer of the Legislature if the information is necessary for the performance of the duties of that officer. *Officers of the Legislature* are the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner and the Information and Privacy Commissioner (**section 1(m)** of the Act).

Disclosure of personal information under **section 40(1)(z)** must be necessary for the performance of the duties of the officer of the Legislature. If the reason for the disclosure is not clear from the request, public bodies should seek an explanation as to why the personal information is needed.

Section 13(1) of the *Election Act* requires the Chief Electoral Officer to establish a register of electors from which lists of electors may be compiled. Section 13(2) states that the register of electors may be created and revised using personal information held by a public body if, in the opinion of the Chief Electoral Officer, the information is necessary for the purposes of creating or revising the register.

In addition, section 13(2.1) requires public bodies to provide personal information from their records to the Chief Electoral Officer, if requested. The information in the register is limited to residential address, mailing address, postal code, surname, given name, middle initial, telephone number, gender, day, month and year of birth and any unique identifier assigned by the Chief Electoral Officer. Public bodies providing this information may charge a reasonable fee for providing the information but the fee may not exceed the actual costs of producing the information.

Section 13(2)(b.1) and section 13(2.1) of the *Election Act* in combination with **section 40(1)(z)** of the *FOIP Act* requires a public body to disclose personal information, as defined in the *FOIP Act*, requested by the Chief Electoral Officer for the purpose of creating or revising the register.

It should be noted that the *Election Act* does not require the disclosure of health information, including health registration information, as defined in the *Health Information Act*, by a public body that is also a custodian under the *Health Information Act*. **Section 40(1)** of the *FOIP Act* permits the disclosure of *personal information*; the Act does not apply to *health information* that is subject to the *Health Information Act* (**section 4(1)(u)** of the *FOIP Act*).

Information may also be disclosed under **section 40(1)(z)** for the purpose of a review of a privacy complaint by the Information and Privacy Commissioner, or an investigation by the Ombudsman at the request of an individual. As with many of the permitted disclosures, a best practice would be to ask the officer to put the request in writing so the public body would have on file a record to support any subsequent disclosure to the officer.

**Disclosure for supervision of an individual by a correctional authority**

**Section 40(1)(aa)** This provision permits the disclosure of personal information about an individual for the purpose of supervising the individual while he or she is under the control or supervision of a correctional authority. The individual may be in a correctional

institution or may be under the supervision of a correctional authority in the community.

If a community service organization is providing services to an individual who is under the control or supervision of a correctional or parole authority, this provision would permit, but not require, a public body, such as Alberta Solicitor General and Public Security, to disclose personal information to the service organization about an individual's history, release or supervision. The information disclosed would have to be necessary for the service being provided. The organization would be prohibited from any subsequent or secondary disclosure of that information, unless the disclosure was authorized by law.

*Supervision* includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of individuals held in a correctional institution.

#### **Disclosure of information available to the public**

**Section 40(1)(bb)** This provision permits personal information to be disclosed when that information is available to the public. It applies to information that has been published in any form or which constitutes or is a part of a record that is publicly available.

The provision covers situations where the information to be disclosed is already in the public domain; the public body need not have necessarily *collected* the information from a public source.

It is important, however, to assess carefully just how public the information is. For example, just because personal information about an individual has been published in the media does not mean that the information should automatically be treated as public and disclosed freely. If a public body is contemplating making this type of disclosure, it should take into consideration the possibility that the individual involved might still find such disclosure an unreasonable invasion of his or her privacy (see *IPC Order 99-032*).

Particular caution should be exercised when disclosing information that is publicly available on the Internet. A public body should ensure that any personal information that it is considering disclosing under **section 40(1)(bb)** was collected in accordance with **section 33** of the Act, that indirect collection was authorized under **section 34(1)** and that, if the information was used to make a decision directly affecting an individual, the public body made every reasonable effort to ensure the accuracy and completeness of the information, as required by **section 35(a)**.

Examples of public information that might be disclosed under this provision include:

- individual employee information in a corporate telephone directory available for purchase or freely available on the Internet;
- biographical information about board appointees published in a newsletter;
- details of a personal service contract approved in a council meeting;
- a retirement notice or information of a school superintendent mentioned in public board minutes; and

- information in court decisions published in law reports (see *IPC Order 98-001*).

**Disclosure of business contact information**

**Section 40(1)(bb.1)** This provision permits a public body to disclose personal information if the personal information is information of a type routinely disclosed in a business or professional context and the disclosure

- is limited to an individual's name and business contact information, including business title, address, telephone number, facsimile number and e-mail address, and
- does not reveal other personal information about the individual or personal information about another individual.

This provision permits, but does not require, public bodies to disclose the names and business contact information of individuals (including e-mail address) if doing so would not reveal other personal information.

For example, a public body may

- publish an employee directory on its website;
- distribute a list of consultants providing professional services in the public body's area of operations, for example, at the request of another public body or a business;
- provide a list of participants in a consultation process involving a public body's business stakeholders; or
- provide a list of e-mail addresses of a public body's contractors and business partners to an IT service provider offering coordinated e-mail service to several public bodies.

For further information see FOIP Bulletin No. 13: *Business Contact Information*, published by Access and Privacy, Service Alberta.

**Disclosure to a relative of a deceased person**

**Section 40(1)(cc)** This provision permits a public body to disclose personal information to the surviving spouse, adult interdependent partner or relative of a deceased individual if, in the opinion of the head of the public body, disclosure would not be an unreasonable invasion of the deceased individual's personal privacy.

*Spouse* refers to a husband or wife of the deceased.

*Adult interdependent partner* means a person who

- lived with the deceased in a relationship of interdependence
    - for a continuous period of not less than three years, or
    - of some permanence, if there is a child of the relationship by birth or adoption,
- or
- entered into an adult interdependent partner agreement with the other person under section 7 of the *Adult Interdependent Relationships Act* (section 3 of that Act).

*Relationship of interdependence* means a relationship outside marriage in which any two persons share one another's lives, are emotionally committed to one another, and function as an economic and domestic unit (section 1(f) of the *Adult Interdependent Relationships Act*). In determining whether two persons function as an economic and domestic unit, a public body must take all the circumstances of the relationship into account. A list is included in section 1(2) of the *Adult Interdependent Relationships Act*.

A *relative* in this context refers to a person connected by blood or marriage such as a mother, father, son, daughter, brother, sister of the deceased and may also include in-laws. Public bodies should consider any relevant guidelines about the interpretation of the term *relative* that may exist in applicable legislation.

**Section 40(1)(cc)** allows the head of a public body discretion to disclose personal information about a deceased individual, taking into consideration both the test for unreasonable invasion of personal privacy (**section 17**) and the relationship between the deceased and the individual to whom the information may be disclosed, including, for example, the relationship of the individual to the deceased at the time of death.

Privacy for a deceased individual normally continues for a period of 25 years (see **section 17(2)(i)**). **Section 40(1)(cc)** permits a public body to disclose information to a relative prior to the expiry of the 25-year period if the disclosure would not be an unreasonable invasion of the deceased individual's personal privacy, taking into consideration the factors in **section 17(5)** and other relevant circumstances.

Particularly important factors to consider are whether

- the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny;
- the personal information is relevant to a fair determination of the requesting individual's rights;
- the personal information was originally supplied by the requesting individual;
- the personal information was supplied in confidence;
- disclosure may endanger the physical or mental well-being of any other living member of the family;
- there are grounds to believe that another member of the family does not want the information disclosed to the relative;
- the personal information is likely to be inaccurate or unreliable;
- the information contains medical, psychological or social work case reports or data which it is reasonable to believe would prove harmful to family relationships; and
- disclosure may harm the reputation of the deceased.





**Evidence of the relationship of the person to the deceased individual should be produced before personal information is disclosed. This should consist of reliable documentation of the relationship (e.g. a birth or marriage certificate). As well, if a public body is not certain that the individual is deceased, the person seeking disclosure must provide reliable evidence that the individual is dead (e.g. a death certificate or obituary notice).**

For further information about disclosure of personal information about deceased persons, see FOIP Bulletin No. 16: *Personal Information of Deceased Persons*, published by Access and Privacy, Service Alberta.

***Disclosure to the legal representative of an inmate***

**Section 40(1)(dd)** This provision permits the disclosure of personal information to a lawyer or student-at-law who is acting for an inmate under the control or supervision of a correctional authority. The disclosure of personal information without the individual's consent may be necessary for the legal representative to properly represent an inmate, for example, in a first appearance hearing.

For information on the meaning of supervision, see the discussion on **section 40(1)(aa)** above.

***Disclosure to avert imminent danger to health or safety***

**Section 40(1)(ee)** This provision permits disclosure of personal information if the head of a public body believes, on reasonable grounds, that disclosure will avert or minimize an imminent danger to the health or safety of any person.

*Imminent danger* means a danger that is likely to arise immediately or very soon.

This provision permits the disclosure of the personal information of *any individual*, not only an individual who endangers health or safety or an individual whose health or safety is endangered. This is one of the few provisions of **section 40(1)** that requires an exercise of discretion by the head of the public body.

The head of a public body will have to consider all the circumstances and all the information in the public body's possession about an individual when making a decision. Past behaviour of the individual is one factor that may assist in decision-making.

Examples of information that might be disclosed under this provision include:

- information about the escape or release of a violent offender to a past victim; and
- information about a student's threat of suicide to residence supervisors on a college campus.

**Disclosure for administration of the Motor Vehicle Accident Claims Act**

**Section 40(1)(ff)** This provision permits disclosure of personal information to the Administrator of the *Motor Vehicle Accident Claims Act* or to an agent or lawyer of the Administrator.

**Section 40(1)(ff)** is intended to allow the Administrator to deal with claims made under that Act. It permits police services and other public bodies, such as Alberta Infrastructure and Alberta Transportation, to disclose any information gathered about an accident to the Administrator once a claim has been lodged.

**Disclosure of alumni records for fund-raising purposes**

**Section 40(2)** This provision permits post-secondary educational institutions to disclose information in their alumni records for the purposes of their own fund-raising activities.

Disclosure may be made to any person acting on behalf of the post-secondary institution in raising funds. This includes alumni associations, foundations, private fund-raising organizations, and other persons raising funds on behalf of the institution. In this context, "person" means a legal entity capable of entering into an agreement.

The person to whom the disclosure is made must have a written agreement with the post-secondary institution. The agreement must

- allow individuals a right of access to their own personal information disclosed under the agreement; and
- provide that the person using the information will discontinue using that information if an individual so requests.

The agreement should also contain other clauses to ensure compliance with the privacy protection provisions of the Act.

**Section 40(2)** is intended for situations where the post-secondary wants to disclose alumni information to a separate, arms-length body. It is not intended for situations where the alumni information is transferred to an office that is *part of* the post-secondary body.

**Section 40(2)** also does not apply where the body is providing services to the post-secondary institution under a contract or agency relationship. In these situations, the post-secondary would retain control of the information.

This provision complements the provision in **section 39(2)**, as outlined in section 7.6 of this chapter. See also FOIP Bulletin No. 5: *Fund-Raising*, published by Access and Privacy, Service Alberta.

**Disclosure of teaching and course evaluations**

**Section 40(3)** This provision permits disclosure of personal information contained in student evaluations of instructors and courses at post-secondary educational institutions.

Disclosure is limited to evaluations completed by students. It does not extend to evaluations of courses by faculty members. The amount of personal information disclosed is limited to that which would assist a student in selecting courses. If the evaluation includes information not relevant to selection of a course (e.g. the

evaluated course is no longer offered or the evaluation is otherwise not current), it cannot be disclosed.



**Post-secondary educational bodies should ensure that information about teaching and course evaluations is valid and up-to-date before it is disclosed, and should establish written policies to ensure that the practice is carried out in a responsible manner.**

#### **Extent of disclosure**

**Section 40(4)** This provision limits the disclosure of personal information to what is necessary to carry out the purposes described in **section 40(1), (2) and (3)**.

For example, a public body communicating the result of an investigation might need to consider whether each party needs all the personal information relevant to the investigation or whether a separate letter or e-mail is required for each party (see *IPC Investigation Report F2004-IR-002*).

The extent of disclosure also arises when there are threads of e-mails. When notifying an employee about an incident, it may not be necessary for the employee to receive the entire chain of e-mails between a complainant and various staff members (see *IPC Order F2005-014*).

#### **7.8 Consistent Purposes**

**Section 41** states that for the purposes of **sections 39(1)(a) and 40(1)(c)**, a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure

- has a reasonable and direct connection to that purpose; and
- is necessary for performing the statutory duties of or for operating a legally authorized program of the public body that uses or discloses the information.

**Section 41** balances the protection of individuals' privacy against the need of public bodies to use and disclose personal information effectively to carry out program activities and fulfil their legislated mandates.

**Section 39(1)(a)** allows a public body to *use* personal information for a purpose that is consistent with the purpose for which the information was originally collected.

In most cases the public body using the information will be the public body that collected it. However, if the personal information has been collected for the purposes of delivering a common or integrated program or service, the public body using the information may not be the public body that originally collected it.

See section 7.7 of this chapter for further information on common or integrated programs and services (**section 40(1)(i)**). See also FOIP Bulletin No. 8: *Common or Integrated Programs or Services*, published by Access and Privacy, Service Alberta.

**Section 40(1)(c)** allows a public body to *disclose* personal information for a purpose that is consistent with the purpose for which the information was originally collected.

In most cases this provision will apply to disclosure outside the public body. The new purpose for using or disclosing must be consistent with the purpose for which the information was collected or compiled.

A use or disclosure has a *reasonable and direct connection* to the original purpose if there is a logical and plausible link to the original purpose. A consistent use should grow out of or be derived from the original use; it should not be an unrelated or secondary use of the information, otherwise known as “function creep.”

A use or disclosure is *necessary for performing the statutory duties of, or for operating a program of, the public body* if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed.

A consistent use or disclosure must meet both of the above conditions to be valid.

### **Examples of a consistent purpose**

#### ***Evaluation of a program***

Public bodies will have a regular need to evaluate the operation and success of their programs. This is particularly true of new programs or those that have changed in some way. **Section 41** allows a public body to select clients or participants who can participate in that evaluation through questionnaires or interviews.

#### ***Verification of ownership***

Local government bodies issue permits for such things as development of a property, demolition and burning. These permits are issued to the owner of a property. **Section 41** allows the staff who approve the permit to verify ownership from the assessment roll.

#### ***Expansion of a program***

Public bodies set criteria for participation in programs. If the criteria are broadened, individuals who were originally rejected may become eligible. This provision allows a public body to determine eligibility on the basis of the original submissions from these individuals rather than collecting the information again. It also enables the public body to do cost projections with respect to the expanded eligibility parameters. Although “dummy” data may often be used for such purposes, there may be times when real or live data is needed.

In *IPC Order 2001-038*, the Commissioner found that a school board’s disclosure of a child’s personal information for the purpose of setting up and administering an e-mail system was consistent with the original purpose for collection – namely, to register the child in school. However, disclosure of that information for advertising, marketing and revenue generation were not consistent purposes.



**Public bodies are required to maintain a record of all uses of personal information, including all consistent uses and disclosures, in order to be able to provide complete, current and accurate descriptions of the personal information banks in their custody or under their control for the use by the public (section 87.1(2)(d)).**

---

**7.9  
Disclosure  
for Research  
or Statistical  
Purposes**

**Section 42** of the Act enables a public body to disclose personal information for a research purpose, including statistical research, only if

- the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the Information and Privacy Commissioner;
- any record linkage is not harmful to the individuals the information is about and the benefits to be derived from the record linkage are clearly in the public interest;
- the head of the public body has approved conditions relating to the following:
  - security and confidentiality,
  - the removal or destruction of individual identifiers at the earliest reasonable time,
  - the prohibition of any subsequent use or disclosure of the information in individually identifiable form without the express authorization of that public body;
- and
- the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, the *FOIP Act* and any of the public body's policies and procedures relating to the confidentiality of personal information.

**Section 42** enables research to take place while at the same time ensuring that privacy is protected. This is accomplished by the strict conditions set out above. Prior to disclosing personal information for research purposes under this provision, a public body must ensure that all four requirements are met.

For a *research purpose* means for the purpose of a systematic investigation or study of materials or sources in order to establish facts or to verify theories.

*Statistical research* is research based on the collection and analysis of numerical data using, in this case, quantifiable personal information to study trends and draw conclusions.

The *FOIP Act* does not expressly prohibit disclosure of information other than personal information for a research purpose under a confidentiality agreement. Public bodies should seek legal advice as to whether disclosure of, for example, confidential third party business information for a research purpose could expose the body to the risk of legal action on the part of the third party.



### Individually identifiable information

Information is in *individually identifiable form* if unique identifiers are attached to the information such that the information can identify a particular individual. The identifiers might be an individual's name, address, telephone number, date of birth or social insurance number. Small population cells or contextual information may also allow for the identification of an individual.

**Section 42(a)** makes provision for situations where

- the research purpose cannot reasonably be accomplished unless the information is provided in individually identifiable form; or
- the research purpose has been approved by the Commissioner.

The first part of this provision allows public bodies to disclose personal information for research in circumstances where the research cannot be completed without access to the information in individually identifiable form. The onus is on the public body to understand research methods generally and the proposed project specifically, to determine whether identifiable information is truly needed to accomplish the research. The second part of the provision allows public bodies to disclose personal information for research if the Commissioner has approved the research purpose. Approval by the Commissioner ensures that the research purpose is subjected to impartial scrutiny.

The researcher would submit the research proposal to either the public body or the Commissioner in writing, clearly explaining the nature of the research, the information involved and the reason for the request. A detailed proposal enables the public body or the Commissioner to evaluate the necessity for identifiable information, any potential harm to individuals, the academic credentials, skill and reputation of the researcher, and proposed security for the records containing the information.

### Record linkage

**Section 42(b)** places controls on any record linkage performed during a research project.

*Record linkage* is a form of data matching involving the systematic comparison of sets of information, often personal, to establish relationships among data. Within the research context, it often involves the creation of a new database allowing the statistical correlation of research variables. Record linkage can be a useful tool for quantitative analysis in research projects.

Record linkage for research purposes is the matching of sets of personal information to achieve the objectives of the research project, generally with no intention of making decisions about the research subjects' rights or privileges. The matching is a means of linking the right information to the right people in a representative sample used in a study. This makes it distinct from the kind of record linkage for individual profiling that is used in some marketing strategies, for example.



**Record linkages permitted under section 42 are only for research purposes and no decision that directly affects an individual may be made as a result of such linkage.**

The provision requires that a linkage *not be harmful*. This means that a linkage must not have an adverse affect on the individuals under study – that is, the information disclosed must not result in damage to an individual's reputation, or denial of a job, benefit or service.

Linkages also need to be considered in terms of the *benefits derived* from them. The benefits of the research and linkage must outweigh the privacy concerns regarding the disclosure of personal information to the researcher. The research and linkage must be clearly in the public interest. That is, the benefits must apply to a wide public and not to just one or two individuals. The written research proposal should outline why this research, using this information, is needed at this time.

### **Approval of conditions**

**Section 42(c)** **Section 42(c)** provides that a disclosure for research purposes may take place only if the public body is aware of and has approved the researcher's proposed practices for handling personal information.

*Security* refers to protecting or guarding the personal information used in a research project from unauthorized access or disclosure, theft or other danger. Good security may require such measures as locked filing cabinets, computer controls and access codes, restricted work areas, and encryption or encoding of data, depending on the sensitivity of the data involved and the threat and risk associated with it.

*Confidentiality* refers to the condition whereby personal information is kept private and safe from unauthorized access, use or disclosure. It means that there is no disclosure, orally or otherwise, other than to those working on the project. For sensitive personal information, disclosure should be on a "need-to-know" basis. Not everyone on the project team would have a need to know all of the information. Data should be accessed and manipulated in a contained setting before being broadly available to the team.

*Removal or destruction of individual identifiers* means the deletion of identifying information, such as name, address, social insurance number or other numerical identifier, or the destruction of the identifiers in whatever way is appropriate to the medium on which the information is stored. This must be done in such a way as to render the information anonymous, for example, by assigning a randomly generated research project identifier in place of the actual individual identifier.

Removal of identifiers is to take place at *the earliest reasonable time*. This will vary with the circumstances of each project and the comparisons the researcher is making between different sets of data. However, the researcher and the public body should agree on a specific date by which time a researcher must strip off all identifiers. This would be when all the different sets of information have been combined and are ready for analysis.

*Prohibition on any subsequent use or disclosure* means a prohibition on any further use or disclosure of the personal information by the researcher for any purpose, including any other research or statistical purpose. The personal information can be used only for the project for which the information was originally disclosed, unless the public body explicitly authorizes another research use. This prohibition includes a ban on the use of the information to sell products or services to the subjects of the study and a ban on the sale or gift of the information to a charity in order to help solicit donations.

### **Agreement to comply with approved conditions**

*Section 42(d)* **Section 42(d)** provides that the researcher must sign a detailed research agreement. This agreement must include all the provisions set out in **section 9** of the FOIP Regulation, namely:

- personal information disclosed can be used only for a research purpose set out in the agreement or for which written authorization has been given by the public body;
- the names of those persons who will be given access to the personal information must be provided;
- the researcher must bind these persons, through an agreement, to adhere to the same conditions as the researcher;
- information must be kept in a secure location;
- how and when the identifiers will be removed or destroyed must be specified;
- contact with the individuals to whom the information relates is prohibited without prior written authorization from the public body;
- no use or disclosure can be made of the information in a form that identifies individuals without prior written authorization from the public body;
- information cannot be used for an administrative purpose directly affecting an individual;
- notification of the public body is required if any conditions of the agreement are breached; and
- failure to meet the conditions may result in cancellation of the agreement and leave the researcher open to charges under **section 92(1)** of the Act.

The public body may want to add audit provisions to the agreement so that the security and confidentiality measures of the researcher can be reviewed.

The model **Proposal for Access to Personal Information for Research and Statistical Purposes Form** and the related **Agreement** in Appendix 5 are suitable for an individual or group of researchers that is not part of any public body. If another public body proposes research, a personal information sharing agreement would likely be more appropriate (see section 9.7 of Chapter 9).

**7.10  
Disclosure of  
Information in  
Archives**

**Part 3** of the *FOIP Act* (**section 43**) provides for the disclosure of information without a FOIP request by the Provincial Archives of Alberta or the archives of a public body.

This section is intended to support research and related activities by allowing access to archival holdings, subject to a limited number of restrictions. **Section 43** is *enabling*. It permits the archives to disclose information under specified conditions; it does not require the archives to disclose information.

The section does not affect access to records that were unrestricted before the *FOIP Act* came into force (**section 3(b)**).

**Section 43** does not apply to records deposited in the Provincial Archives of Alberta or the archives of a public body by or for a person or entity other than a public body (**section 4(1)(j)**). These are generally referred to as *private records*. For example, if an individual has made a gift of records to the Provincial Archives, subject to an agreement with respect to access, the *FOIP Act* does not prevent the Provincial Archives from complying with the terms of that agreement.

**Section 43(1)** applies to all public body archives.

**The Provincial Archives of Alberta or the archives of a public body**

The role of the Provincial Archives of Alberta and other public body archives is to select, preserve and make available the non-current records of public bodies that have been preserved because of their enduring value. This includes legal, evidential, financial, and historical value.

The *archives of a public body* means an agency, other than the Provincial Archives of Alberta, that is authorized to perform archival functions on behalf of that public body.

The archives of a public body may be

- a public body's own archives, in which case the records will remain in the custody or under the control of that public body (e.g. the archives of most post-secondary institutions);
- the archives of another public body, to which records may be transferred under **section 3(e)**, in which case the records will normally be in the custody and under the control of the archives; or
- an archival facility that operates under a contract or agency relationship with the public body, in which case custody may be transferred but control must be retained.

The Provincial Archives of Alberta and the archives of public bodies may disclose information, including personal information, in their records, subject to certain conditions set out in **section 43(1)(a)** and **(b)**.

**Disclosure of personal information**

**Section 43(1)(a)** This provision supplements **section 40(1)**, which also allows for the disclosure of personal information without a FOIP request. Disclosure under this provision depends upon the age of the record.

If personal information is in a record that is *less than 25 years old*, the archives cannot disclose it under **section 43(1)(a)**. The archives must either apply a relevant provision in **section 40(1)**, such as disclosure in accordance with an enactment that authorizes or requires the disclosure (**section 40(1)(f)**), or ask the person seeking the information to submit a FOIP request.

If the personal information requested is in a record that has been in existence for *25 years or more*, the archives may disclose the information under **section 43(1)(a)** if the disclosure

- would not be an unreasonable invasion of privacy under **section 17**; or
- is in accordance with **section 42** (which specifies conditions for disclosure of personal information for a research purpose).

Section 4.3 of Chapter 4 sets out guidelines for applying **section 17**.

If the personal information is about an individual who has been dead for 25 years or more, and satisfactory proof of that fact is provided, disclosure would not be an unreasonable invasion of privacy under **section 17(2)(i)** and the personal information may be disclosed under either **section 43(1)(a)(i)(A)** or **section 40(1)(b)**.

If the person requesting disclosure cannot prove that the individual has been dead for at least 25 years, and it is determined, after application of the other provisions of **section 17**, that the disclosure would be an unreasonable invasion of a third party's privacy, the archives can disclose the information only in accordance with **section 42**, which requires a research agreement.

Information about research agreements and the application of **section 42** is provided in section 7.9 of this chapter. If disclosure is made under **section 42**, the archives must have a written agreement in accordance with **section 9** of the FOIP Regulation.

If the personal information is in a record that has been in existence for *75 years or more*, the archives may disclose that information without restriction under the *FOIP Act*.

Disclosure under **section 43(1)(a)** may be subject to the restrictions of legislation that is paramount over the *FOIP Act*. The effects of other Acts is discussed at the end of this chapter.

#### ***Disclosure of information other than personal information***

**Section 43(1)(b)** This provision allows archives to disclose information, other than personal information, in a record that is 25 or more years old. **Section 43(1)(b)** supplements **section 88**, which allows the heads of public bodies to specify certain categories of information that may be made available to the public without a FOIP request.

**Section 43(1)(b)** is intended to establish greater transparency for archives, which tend to hold large volumes of records collected by public bodies. This transparency benefits not only public bodies that transfer the custody and control of their records to archives, but also the researchers who use the collections.



**Section 43(1)(b)** requires the Provincial Archives or the archives of a public body to assess the information that is being considered for disclosure and determine whether disclosure could still result in harm or whether disclosure may be prohibited for some other reason.

Information may be disclosed under this provision if

- disclosure would not harm the business interests of a third party within the meaning of **section 16**;
- disclosure would not harm a law enforcement matter within the meaning of **section 20**; and
- the information is not subject to any type of legal privilege under **section 27**.

Details on the application of **section 16** are provided in section 4.2 of Chapter 4. If the information is in a record that has been in existence for 50 years or more, then **section 16** does not apply.

Details on the application of **section 20** are provided in section 4.6 of Chapter 4.

Details on the application of **section 27** are provided in section 4.13 of Chapter 4.



As a best practice, when public bodies transfer records to archives, they should identify any records that may be subject to restrictions imposed by other Acts. They should also identify any records to which the exceptions in the *FOIP Act* for disclosure harmful to the business interests of a third party or harmful to law enforcement may apply, as well as any records that may be subject to legal privilege (where known).

Accepted archival practice involves the accessioning of records according to organizational principles and standards that assist researchers in using the records. Archives may find it helpful to have policies in place that explain the relationship between their procedures and practices and the provisions of the *FOIP Act*. For example, if it is decided to apply **section 43(1)** to open a particular collection in the archives, the policy may set out the criteria that are used to determine that information in the record series meets the test of being 25 or more years old.

### Effect of other Acts

Archives may disclose information in records as described above provided the information is not subject to a confidentiality provision of another Act or regulation of Alberta that is paramount over the *FOIP Act* or an enactment of Canada that is paramount over the *FOIP Act* (by virtue of federal paramountcy).

**Section 5** of the *FOIP Act* provides rules for applying the Act when the relationship between the *FOIP Act* and another enactment does not allow both to operate in their entirety at the same time. If another Act or a regulation under the *FOIP Act* expressly states that a provision of another enactment prevails despite the *FOIP Act*, the *FOIP Act* does not apply. The other enactment applies, on its own terms.

If a provision of the *FOIP Act* is inconsistent or in conflict with a provision of another enactment, and neither the other Act nor the FOIP Regulation says that the other provision prevails despite the *FOIP Act* the *FOIP Act* prevails to the extent of the inconsistency.

This provision is particularly significant for archives because much of the legislation prohibiting disclosure of information that is paramount over the *FOIP Act* does not set time limits on the prohibition. For example, there are no time limits on the prohibitions on disclosure in the paramount sections of the *Child, Youth and Family Enhancement Act* or the *Maintenance Enforcement Act*.



**Public bodies transferring records to archives should identify any records that are subject to any restriction or prohibition on disclosure under legislation that is paramount over the *FOIP Act* and any time limits that apply.**

For further information on the effect of paramountcy, see FOIP Bulletin No. 11: *Paramountcy*, published by Access and Privacy, Service Alberta.

#### 7.11 Record of Purposes

Public bodies should ensure that all uses and disclosures of personal information that are routine in nature and occur frequently are described in generic terms in the description for the appropriate personal information bank in the directory of personal information banks. This fulfils the requirement set out in **section 87.1(2)(d)** to notify the public about such uses and disclosures. Public bodies must ensure that the directory is kept as current as is practicable, and that access to the directory is available to the public at an office of the public body, or on the public body's website (**section 87.1(4)**).

**Section 87.1(3)** Under this provision, if personal information is used or disclosed by a public body for a purpose that is not included in the directory of personal information banks, the head must

- keep a record of the purpose and either attach or link that record to the personal information; and
- ensure that the purpose is included in the next publication of the directory.

There are a number of ways to meet the requirement to attach or link a record of purpose to the personal information. For paper files, when the request is for information about one or more individuals, a copy of the official request for use or disclosure of the personal information, together with the signature of the official or employee agreeing to such use or disclosure, can be attached to individual files. When the request is for a large number of files, a control file can be created, containing the same information.



**If an individual whose information is contained in the file series requests his or her personal information, the part of the control file containing information about the individual must be considered for disclosure along with the other personal information.**

If the use or disclosure involves computer files, a tag or other indicator should be inserted in the system linking the user to information regarding the request for and decision to allow the use or disclosure. The requirement to consider the disclosure of information in a control file applies in this case as well.

For further information on directories of personal information banks, see section 2.7 of Chapter 2 and the *Guide to Identifying Personal Information Banks*, published by Access and Privacy, Service Alberta.







## 8.

**RECORDS AND INFORMATION MANAGEMENT****Overview**

This chapter is intended to help public bodies understand how good records and information management practices assist in the effective administration of the *FOIP Act*.

All types of organizations, including public bodies, manage their recorded information for reasons that are significantly broader than compliance with access and privacy legislation: they create, maintain and manage records to provide tangible evidence of their business activities and transactions.

The primary purposes for records and information management are to

- support policy formation and managerial decision-making;
- improve client services and support better performance of business activities;
- support consistency, continuity and productivity in operations, administration and management;
- protect the interests of the organization and the rights of clients, the public and employees;
- provide protection and support in litigation, including the better management of risks associated with the existence or lack of evidence of activities or events;
- facilitate research and development activities; and
- enable organizations to meet legislative and regulatory requirements.

Also, to meet their obligations under the *FOIP Act*, public bodies need to have in place effective records and information management practices. Such practices should be modelled on national and international standards such as:

- International Standards Organization Records Management Standard (ISO 15489);
- Canadian General Standards Board standards for documentary evidence; and
- ARMA International's standards and guides (see [www.arma.org](http://www.arma.org)).

**8.1  
Scope**

Service Alberta administers the records management program in government. Alberta government departments, boards and agencies subject to the Records Management Regulation (AR 224/2001) must adhere to the policies and guidelines established under this Regulation.

For provincial government departments and their affiliated agencies, boards and commissions (FOIP Regulation **Schedule 1** public bodies), this chapter supplements the policies and guidelines issued by Service Alberta.

More detailed information on records and information management practices may be obtained from publications produced by Records and Information Management, Service Alberta ([www.im.gov.ab.ca](http://www.im.gov.ab.ca)), such as:

- *Information Assets in the Government of Alberta: A Management Framework*
- *Information Management Planning*
- *Information Security Classification*
- *Official and Transitory Records: A Guide for Government of Alberta Employees*
- *Developing Records Retention and Disposition Schedules*
- *Managing Electronic Mail in the Government of Alberta*
- *Managing Instant Messages in the Government of Alberta*

Local public bodies are not subject to the provincial Records Management Regulation. Under **section 3(e)(ii)** of the *FOIP Act*, regulation of records management in local public bodies must be by bylaw, resolution or other legal instrument by which a local public body acts, or, in the absence of such a legal instrument, as authorized by the governing body of the local public body.

Records scheduling and disposition in local public bodies should be based on recognition of the role of records management in effective public administration. In particular, local public bodies should be aware of the importance of an authorization process for the disposition of records that ensures that the local public body can meet its financial and legal obligations, including its obligations under the *FOIP Act*.

---

## **8.2 Powers of the Commissioner**

**Section 53(1)(a)** of the Act authorizes the Information and Privacy Commissioner to monitor the general administration of the *FOIP Act* to ensure that its purposes are achieved. This includes conducting investigations to ensure compliance with rules relating to the destruction of records set out in

- any other enactment of Alberta;
- a bylaw, resolution or other legal instrument by which a local public body acts; or
- any rules relating to the destruction of records that are authorized by the governing body of a local public body.

Public bodies, therefore, should expect their records and information management practices to be under scrutiny during reviews, investigations and privacy audits conducted by the Commissioner's Office. This is especially the case when an applicant requests a review of the adequacy of a search for information or records.

---

## **8.3 Records and Information Management Principles**

The following principles underpin the effective management of recorded information.

### **Information is an important asset of the organization**

An essential principle for the management of recorded information is that information is managed as a resource or asset of the whole organization and not as the property of individuals, branches or divisions.

### **The management of information is planned**

An organization's business planning processes require both strategic and operational records and information management planning.

### **A life-cycle management approach is adopted**

Sound principles for the management of recorded information are based on the life cycle of information. Management activities within the life cycle encompass

- the planning of information systems, including appropriate controls over the collection, creation or compilation of recorded information;
- the establishment of practices and procedures governing the organization, distribution, retrieval, use, accessibility, and transmission of the recorded information and for its storage, maintenance and protection;
- provision for routine disclosure and dissemination of such information, as appropriate; and
- the regulation of the scheduling and disposition of all recorded information.

### **All records are included**

Management practices should apply to all records as defined in the *FOIP Act*, including personal information and electronic records.

Electronic records include

- electronic documents, such as word processed documents, e-mail, web pages, graphics, digital photographs, and scanned images; and
- electronic data, such as information stored in databases.

Electronic records include information in all media and in all locations. For example, electronic records may be stored on networks, local hard drives, portable hard drives, and personal digital assistants, as well as in portable storage devices, such as CDs, USB drives, DVDs, and tapes.

### **Accountability is assigned**

In the case of provincial government departments and FOIP Regulation **Schedule 1** public bodies, the Records Management Regulation assigns accountability for records management in the public body to the deputy head.

Given the close relationship between the *FOIP Act* and the effective management of recorded information, there should be a similar assignment of accountability for the management of recorded information in local public bodies.

**8.4  
Records and  
Information  
Management  
Policy  
Components**



**Policies and guidelines should govern the management of recorded information in a public body.**

Policies and guidelines should be developed with the administration of the *FOIP Act* in mind and should include appropriate references to access to information and protection of privacy requirements in policy statements, procedures, practices and standards.

The following components should be included in policies and guidelines for the management of recorded information:

- life-cycle management of recorded information;
- establishment and maintenance of a records system;
- a guide to personal information banks;
- guidelines for the creation and generation of records;
- a guide for transitory records;
- records management in contracting;
- scheduling and disposition of recorded information;
- guidelines and practices relating to the retention and disposition of e-mail and other forms of electronic messages;
- rules for the organization, storage and protection of recorded information;
- rules for the organization and management of electronic records;
- records system requirements for planning and designing electronic applications that will collect, create or generate information used by the public body; and
- security.

**Managing recorded information throughout its life cycle**

A public body should plan, direct, organize and control recorded information throughout its life cycle, regardless of the form or medium in which the information is held.

**Establishing and maintaining a records system**

A records system, which may be computerized or manual, is an information system that captures, maintains, manages and provides access to records over time. Increasingly, organizations are implementing specialized electronic records and document management technologies to support this function.

A records system should be controlled by a current and comprehensive classification structure, to arrange, locate and retrieve recorded information in the custody or under the control of the public body. The classification structure should link to the organization's records retention and disposition schedules to facilitate effective disposition practices. For provincial government departments and FOIP Regulation **Schedule 1** public bodies, the *Administrative Records Disposition Authority (ARDA)*

and the *Transitory Records Retention and Disposition Schedule*, published by Records and Information Management, Service Alberta, are generally used for the disposition of administrative and transitory records respectively.

The records system should serve as a locator system for all holdings of recorded information. It should also identify the business unit responsible for particular information holdings. In addition, it should support the application of privacy protection measures and support vital records identification for business resumption planning purposes.

### **Establishing and maintaining a directory of personal information banks**

**Section 87.1(1)** requires the head of a public body to publish a directory, in printed or electronic form, listing the public body's personal information banks (PIBs). This applies to government departments and **Schedule 1** public bodies, as well as to local public bodies. For government departments and **Schedule 1** public bodies, personal information banks are identified in records schedules. **Section 87.1(2)** sets out the elements that must be included in the directory for each PIB.

For more information on PIBs, see *Guide to Identifying Personal Information Banks*, published by Access and Privacy, Service Alberta.

For more information on directories of records, see section 2.7 of Chapter 2.

### **Creating, maintaining and using records**

Effective controls over the creation, maintenance and use of recorded information in the conduct of the business of the organization should be established through a written guideline.

The guideline should indicate what records need to be created and maintained. For example, records required for legal, fiscal, audit, administrative or operational purposes should be retained in a records system. For a discussion of what records should be created, which records should be retained and filed, and which records can be routinely destroyed within the Government of Alberta, see *Official and Transitory Records: A Guide for Government of Alberta Employees*, published by Records and Information Management, Service Alberta.

Any established guideline should be understood and followed by all public body officials and employees.

### **Scheduling and disposing of recorded information**

Control over the disposition of recorded information is an important aspect of records and information management that is critical to FOIP administration. When responding to a FOIP request, it is necessary to know whether records have been destroyed and if so, whether this has been done in an authorized manner.

It is equally important to dispose of personal information under conditions that protect the privacy rights of the individual. Records retention and disposition schedules are a public body's legal authorities on how long recorded information



must be kept and how it is to be disposed of, e.g. by destruction or archival preservation.



**Each public body should establish a scheduling process that governs the retention and final disposition of all the recorded information in its custody or under its control.**

For public bodies subject to the Records Management Regulation, the Alberta Records Management Committee approves records retention and disposition schedules. The schedules provide authority to transfer inactive records to off-site storage, for destruction of records, and for the transfer of records selected for archival preservation to the Provincial Archives of Alberta. See also the Government of Alberta's Transitory Records Schedule under the Records Management Regulation.

The scheduling process and guidelines for the transfer and destruction of records are discussed in *Developing Records Retention and Disposition Schedules*, published by Records and Information Management, Service Alberta, and in related Alberta Records Management Committee Circulars.

### **Securely disposing of personal information**

*Authorized disposition* of personal information may occur through

- transfer of records to the custody of the Provincial Archives of Alberta or the archives of a public body;
- physical destruction of records containing personal information in such a way that it cannot be retrieved or reconstructed; or
- alienation of records as a result of a privatization arrangement or the transfer of service delivery to another body. This disclosure must be authorized by law (a public body that is subject to the Records Management Regulation must have a Records Alienation Schedule approved by the Alberta Records Management Committee to authorize the transfer of records to a non-provincial government organization).

For other public bodies, authority to approve the transfer or destruction of the public body's recorded information will come from its governing body. A public body may have its own archives, or may select the archives of another public body or another archival facility to act for it.

Public bodies must pay strict attention to disposition processes for records. This is true for all recorded information, but particularly so for personal information. Disposal and preservation should be governed by well-documented and well-understood procedures. Commercial pulping or shredding is the best way of disposing of paper and other hard copy media. This should be done using equipment or in a facility that can ensure complete and secure destruction.

All too often, sensitive personal information intended for destruction is left in unsecured conditions and may be exposed to unauthorized access and, possibly, use. Examples include disposal of documents containing personal information in garbage

bags that have ripped open and disposal of personal information in a recycling container.

In *IPC Investigation Report 99-IR-003*, it was noted that the method of recycling that had been used was inappropriate since it exposed employees of the public body and citizens to the risk of misuse of their personal information.

### **Securely disposing of electronic records**

Used office and computer equipment poses a special risk. In one investigation by the Information and Privacy Commissioner, filing cabinets were found to have been moved to an auction centre with files containing personal information still inside. Computer hard drives have been similarly put up for auction with information still stored on them.

At a minimum, computer hard drives need to be professionally wiped clean of data before they are disposed of or sold. See *Security Policy for Disk Wiping Surplus Computers*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta.

#### **Provincial government departments and FOIP Regulation Schedule 1 public bodies are required**



- to have operable hard drives wiped of all data by the ministry in accordance with specified procedures prior to sending the computers to Surplus Sales in Service Alberta; and
- to remove and destroy the hard drives in all computers to be surplus outside the government, except for those to be reallocated to the Computers for Schools program.

Care should also be taken in the return or disposal of devices, such as facsimile machines, scanners and photocopiers, that retain information in memory.

For public bodies subject to the Records Management Regulation, destruction of information must take place in accordance with the records management policies and procedures established by the Government of Alberta. Surplus Sales, Service Alberta offers services to these public bodies for the wiping clean of computer hard disks before their disposal.

See *Policy for Maintaining Security of Government Data Stored on Electronic Data Storage Devices* and *Security Policy for Disk Wiping Surplus Computers*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta.

### **Disposing of transitory records**

A policy, records schedule, bylaw or other instrument should set rules for retention and disposition of records, including transitory records, so individual employees can decide which records should be retained and which records can be destroyed.

A *transitory record* is a record that has only immediate or short-term usefulness or value and will not be needed again in the future. Transitory records contain information that is not required to meet legal or financial obligations or to sustain administrative or operational functions, and has no archival value.

Transitory records are defined for provincial public bodies in the Transitory Records Schedule, approved under the Records Management Regulation. Guidelines for retention and disposition of transitory records can be found in *Official and Transitory Records: A Guide for Government of Alberta Employees*, published by Records and Information Management, Service Alberta.

Local public bodies may develop and approve their own definitions, but must be prepared to explain to the Commissioner why they believe that certain records are transitory records.

Some examples of recorded information that may be managed as transitory records are

- information of short-term value (e.g. personal messages, notes kept to prepare official minutes of a meeting);
- duplicate documents (where nothing has been added, changed or deleted; the copies have been used for reference or information purposes only; and the master version of the document has been filed in an official filing system);
- draft documents and working materials that are used to create a master record, except for drafts of legislation, legal documents, budgets, policy changes or changes in decisions;
- advertising material (including spam);
- external publications;
- e-mail containing personal messages and routine announcements, but not recommendations, decisions or transactions by public bodies. Public bodies should have an internal e-mail policy that aids officials and employees in deciding when e-mail messages should be retained in records systems; and
- voice-mail messages, unless it is necessary to document a decision or transaction recorded on voice-mail.

### **Organizing, storing and protecting recorded information**

A policy that establishes a records system will provide a framework for the organization and storage of recorded information that facilitates the location and retrieval of the information. The policy should also address information security and the protection of personal information, both for business and FOIP purposes.

The public body should have guidelines and procedures in place relating to the organization, control, storage, and protection of recorded information, including electronic records. *IPC Order 2000-020* states that a public body must have an adequate records management system in place to keep track of all internal uses and external disclosures of records and information as part of its duty to protect personal information.

For government public bodies, see also *Government of Alberta Information Technology Security Policy* and *Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta, as well as *Managing Electronic Mail in the Government of Alberta*, published by Records and Information Management, Service Alberta.

### **Organizing and storing electronic records**

Electronic records include both data-based records (i.e. numbers and text in structured fields of databases) and document-based records (i.e. correspondence created in word processing or other applications, web pages, graphical objects and e-mail). Electronic records are subject to the *FOIP Act* and should be managed throughout their life cycle as part of any program for the management of recorded information.

Ideally, in an electronic records system, processes should be in place to ensure that

- individual records are uniquely identified;
- contextual data, or “metadata,” relating to the specific record or transaction is preserved (this may consist of, for example, date, subject, names of correspondents or participants);
- records can be authenticated;
- there is version control;
- records are classified and indexed for retrieval;
- there are access controls;
- there are controls over the alteration of records;
- there is the ability to audit access to and alteration of records; and
- there are processes in place to permit the disposition of records, including e-mail, under approved records schedules using secure processes.

If the public body does not have an adequate electronic records system, its records management policy should require records to be printed and managed as part of the records system used to manage hard-copy records.

Provincial government departments and **Schedule 1** public bodies may refer to *Managing Electronic Mail in the Government of Alberta*, published by Records and Information Management, Service Alberta, for further information and assistance.

### **Including routine disclosure practices and privacy requirements in the planning and design of electronic information systems**

There are two special needs of public bodies that require special information management standards and specifications. These should be considered in the design of electronic information systems.

First, routine disclosure of recorded information outside the *FOIP Act* should be supported. Recorded information should be managed to promote public access where this is appropriate. It may be desirable that electronic information systems include a

public access component. Public bodies should ensure that opportunities for routine access are considered in the design and functional specifications for new or modified electronic information systems. This will facilitate routine disclosure and active dissemination of information, where appropriate, after the system is implemented.

Second, privacy protection measures must be considered in the design and functional specifications for information systems that are used to collect, generate, manipulate, and disclose personal information. The particular requirements for protection of privacy in this area are discussed in Chapter 9.

### **Managing recorded information in contracting**

When public body programs or services are provided by contractors or other agencies, a policy for managing recorded information should state that all contracts require the contractor to create records that meet the public body's requirements.

Contracts should also require the contractor to maintain records according to standards acceptable to the public body for as long as required, to dispose of the records according to standards acceptable to the public body, or to return records to the public body, as appropriate.

When activities requiring the collection or handling of personal information are contracted out, the contract should set out the privacy protection and security obligations assumed by the contractor (see Chapter 9).

Conditions governing FOIP and records management as they relate to contracting are further explained in the publication *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

---

#### **8.5 Records Issues Relating to Access Requests**

The right of access to records provided in the *FOIP Act* is intended to make public bodies more open and accountable to the public. Inadequate record-keeping can contribute to poor accountability to clients and the general public.

In the case of FOIP requests, a public body may find that poor records and information management can cause it to contravene the Act. This may lead to damage to the public body's credibility and reputation. Some common issues that arise in the context of access requests are the ability to locate records, adequate standards of documentation, disposition of records, and disclosure outside the Act.

#### **Ability to find records**

The access provisions of the *FOIP Act* assume that public bodies can identify, locate and produce records in response to requests. This ability is crucial both in making information routinely available to the public and in responding to FOIP requests.

The search process is greatly facilitated if a retrieval system is in place that allows staff processing an access request to search for a particular topic or subject and find all locations where records may be kept and also find the records in any media.



The failure to capture records in effective records systems is the most commonly cited problem associated with inadequate management of records and information. (See, for example, *IPC Order 97-019* and *IPC Investigation Report 98-IR-009*.)

This failure may result in difficult and time-consuming searches for records, as well as uncertainty that all records relevant to a FOIP request have been located. This is particularly an issue when no records can be found on a subject, although it appears that a public body should have created and maintained records on the subject and there is no evidence that the records were disposed of in an authorized manner.

Applicants frequently challenge the adequacy of a search for records by a public body. Public bodies will find it easier to demonstrate thoroughness if there is an established records system. For an example of the analysis of a public body's records system and its search for apparently missing records, see *IPC Order 98-003*.

Public bodies also need to be able to show that a search for records has been conducted in a systematic and reasonable manner. The Information and Privacy Commissioner has stated that a search that relies solely on the memory of an employee is not in compliance with the Act (see *IPC Order 99-021*). The Commissioner has also ruled that a limited "keyword" search does not constitute an adequate search (see *IPC Order 99-002*), and that public bodies should be able to locate all records that are "reasonably related" to the applicant's request (*IPC Orders 97-020* and *99-002*).

On the other hand, a public body is not required to inform an applicant of the existence of records in other public bodies, to provide indexes to files that have not been requested, or to provide an applicant with records retention and disposition schedules (unless this is part of the access request) (see *IPC Order 99-039*).

An effective records system should allow retrieval of semi-active as well as active records (see *IPC Order 96-021*). It should also allow retrieval of inactive records in a storage facility, such as the Alberta Records Centre (for provincial government departments and **Schedule 1** public bodies). The Commissioner has found that there may be a requirement to search and access electronic back-up tapes, depending on the circumstances of a case (*IPC Order F2007-028*).

In addition, the records system should provide some ability to alert an applicant to the fact that records may have been transferred to the public body's archives (see *IPC Order 96-022*).

In *IPC Order 2000-020*, the Commissioner stated that adequate records management under the Act involves keeping track of all internal uses and external disclosures of records and information relating to clients' medical information. In that Order, the Commissioner suggested that the public body should have kept a precise list of the medical records that were provided or summarized for a consultant's review in evaluating a compensation claim.

### **Adequate documentation**

Employees of public bodies are accountable for documenting their activities or transactions. Although the *FOIP Act* does not impose requirements as to how a public body should structure or maintain its records system (see *IPC Order 2000-030*), a public body should have clear direction from senior management as to how officials and employees will document business activities of the public body.

As well, there is a need in the modern electronic work environment to ensure version control, so that public bodies can retrieve the authoritative versions of documents. If information technology systems do not have version control capability, practices should be developed to identify authoritative versions of documents.

This kind of direction may help to reduce situations where records are not created to a standard adequate for the public body's needs or where it is impossible to determine the authoritative version of a record on which a decision or other action was based.

There is also need for clear direction on what records the public body considers to be transitory. In the absence of such direction on transitory records, the Commissioner may require a public body to produce other evidence at an inquiry that a record that has been destroyed was appropriately destroyed as a transitory record (see *IPC Order 99-009*). Transitory records are discussed in greater detail in section 8.4 of this chapter.

Finally, guidelines for employees should clearly indicate that the official records of the organization cannot be altered or destroyed without authorization. Alteration or destruction of records is a very serious matter, especially when done to evade a FOIP request, and could lead to penalties or sanctions. See Chapter 2, section 2.11 for information on the offence provisions of the Act.

### **Controls over disposition**

Cost-effective business practices include having a systematic process for evaluating and disposing of records as they become inactive and are no longer needed for business purposes, for the operations of the public body (e.g. to protect the public body's interests in the event of litigation) or for long-term preservation. Establishment of records retention and disposition schedules, and compliance with them, allows public bodies to set accurate limits to searches for records.

This process, known as records scheduling and disposition, has several advantages from a FOIP perspective. First, properly authorized retention and disposition schedules provide an official approval process for the destruction of records, including transitory records, based on business needs. Schedules also provide evidence for the applicant, and for the Commissioner if necessary, that records have been appropriately disposed of by the public body.

The Commissioner has emphasized the importance of rules relating to the destruction of records, and he has noted that it is within the purview of the Commissioner to ensure compliance with such rules (see *IPC Order 98-011*).

Second, schedules identify what records of enduring value should be transferred to the Provincial Archives of Alberta or other archives. See section 7.7 of Chapter 7 for

a discussion on disclosure of personal information to archives, including the transfer of information to an archival facility that is not a public body, but which has a contract or agency relationship with a public body (**section 40(1)(p)**). FOIP requests can then be dealt with on behalf of the public body by these organizations, which are usually well-placed to deal with requests for records.

Third, schedules allow for the movement of records as their value changes. This reduces the need for public bodies to tie up resources in the maintenance of older records, which may be very labour-intensive to locate and handle. Older records that are needed to record the activities of a public body, to protect its interests or to provide long-term corporate memory for the public body can be placed in the Provincial Archives of Alberta, the archives of a public body, or other archival facility, as appropriate.

Fourth, schedules provide controls over the disposal or destruction of records, so that public bodies know what was destroyed, and when. Adequate documentation related to the destruction of records may also provide useful documentary evidence in the event of a Commissioner's review. In *IPC Order 99-021*, the Commissioner noted that, if records have been destroyed in accordance with approved records retention and disposition schedules, the public body must inform the applicant of the relevant destruction certificate numbers in its response.

#### **Ability to routinely disclose records outside the FOIP process**

A public body needs to have effective control over the records and information it collects and creates and to be knowledgeable about such records and information. This is required to make effective decisions about which records should either be released on a routine basis or actively disseminated to the public.

Routine disclosure and active dissemination are practices that contribute significantly to openness in public administration, better client service and more effective mechanisms to reduce the number of FOIP requests under **Part 1** of the Act. For further information on routine disclosure of records and information, see section 2.4 of Chapter 2.









## 9. PRIVACY COMPLIANCE

### Overview

This chapter covers

- privacy compliance reviews;
- privacy considerations when planning or implementing new or modified programs, information systems or administrative practices;
- privacy impact assessments;
- reviewing forms and other collection instruments;
- developing security policies;
- conducting threat and risk assessments; and
- privacy considerations for data matching and data sharing arrangements.

### 9.1 Privacy Compliance Reviews

Compliance with **Part 2** of the *FOIP Act* can be determined by reviewing a public body's practices, activities, programs and systems in which personal information is collected, maintained, used and disclosed. A privacy compliance review process will assist program managers and administrators responsible for personal information banks in assessing their current level of compliance and in identifying necessary and appropriate steps to bring the public body into compliance, if required.



**Public bodies should have policies and organizational structures in place that will facilitate the integration of privacy protection requirements and practices into the ongoing management of personal information banks, programs, activities and information systems.**

The privacy compliance review process will

- support the public's right to know what personal information the public body is collecting and how this information is used;
- support the right of individuals to access their own personal information;
- assure individuals that their personal information will be collected, used and disclosed only as authorized; and
- maintain public confidence in the public body's systems and programs with respect to the handling of personal information.

The following framework, based upon the applicable *FOIP Act* sections, can be used to review how a program, activity or information system protects personal information.

### **Protection of personal information analysis**

**Sections 33 to 42** of the *FOIP Act* control the manner in which personal information is collected, used and disclosed and the requirements for protecting, correcting, retaining and assuring the accuracy of such information. This framework identifies what a public body is required to do under the Act and also, in some instances, what a public body may want to consider doing in addition to what is required under the Act. **Part 2** of the Act and Chapter 7 should be referred to while using the framework.

### **Authority for collection**

**Section 33** **Section 33** limits the collection of personal information by public bodies. Collection must be authorized under **section 33(a), (b) or (c)**.

#### ***What is required?***

- An enactment of Alberta or Canada must specifically authorize collection of the personal information; that is, the enactment must expressly refer to the activity of collecting personal information for specified purposes; or
- The personal information must be collected for the purposes of law enforcement; or
- The personal information must relate directly to and be necessary for an operating program or activity of the public body (the collection cannot be for a prospective program or activity that does not currently exist and personal information must not be collected “just in case”).

#### ***For consideration***

- When establishing new programs or reviewing existing programs and activities, consider putting a process in place to ensure that the minimum amount of personal information necessary to carry out the program or activity is collected.

### **Manner of collection**

**Section 34(1)** **Section 34(1)** requires a public body to collect personal information directly from the individual the information is about except in certain limited circumstances.

#### ***What is required?***

- Personal information must be collected directly from the individual the information is about (direct collection) unless the public body is authorized to collect information indirectly.
- If the personal information is collected from a source other than the individual the information is about (indirect collection), there must be authority in **section 34(1)(a) to (o)** for indirect collection.

If a public body is not authorized to collect personal information indirectly under **section 34(1)(a) to (o)**, the public body must either collect the personal information directly from the individual or not collect the personal information at all. The only

exception to this would be if **section 34(3)** applies (information collected directly would be inaccurate).

#### **For consideration**

- **Section 34(1)(a) to (o)** permits indirect collection in a number of different circumstances. However, a public body should consider collecting personal information directly unless indirect collection is necessary in the specific circumstances of the program or activity.

#### **Notification of collection**

*Section 34(2)* When personal information is collected directly from an individual, notification of the purposes of and authority for the collection must be provided to the individual.

#### **What is required?**

- If personal information is collected directly, the notification provided to the individual from whom the information is collected must include
  - the specific purposes for which the information will be used;
  - the specific legal authority for the collection of information (the public body's own governing legislation or the *FOIP Act*); and
  - the title, business address and telephone number of an official in the public body who can answer questions about the collection of personal information.
- If notification is not given to the person from whom the information is collected,
  - one of the paragraphs in **section 34(1)(a) to (o)** must apply; or
  - the head of a public body must have decided that the direct collection requirement or the notification requirement could reasonably be expected to result in the collection of inaccurate information.
- The method of notification must be appropriate in the circumstances. Examples of different methods of notification include notice on a form, in a pamphlet or other publication, on a card or sign on a desk or counter, on a website, or in a pop-up notice on a computer screen. Oral notice can be given either in person or by recorded message.

#### **For consideration**

- Consider whether a client may need to refer to the information in the notice in the future or whether the program area may need to retain evidence of the notice that was given. In these cases, provide a copy of the notification to the individual from whom the personal information is collected and keep a copy of the notification on file.
- Consider providing notification even in cases where a public body is not required to do so (that is, in cases where the public body is authorized to collect personal information indirectly). For example,
  - In cases where a public body collects personal information indirectly for the purpose of a common or integrated program or service, consider notifying the client of the collection of his or her personal information by

the various public bodies that are involved in the delivery of the program or service, at the time a client registers in the program or requests the service.

- In cases where a public body collects personal information indirectly for the purpose of determining the suitability of an individual for a scholarship or bursary, consider notifying the individual what information will be collected and from whom, at the time the individual applies for the scholarship or bursary.
- Consider the most appropriate methods of providing notification for collection of personal information by telephone or electronically. For oral collection, consider having a policy on providing notification (e.g. recording on client files that notice has been provided), and monitoring compliance.

### **Accuracy of personal information**

**Section 35(a)** A public body must make every reasonable effort to ensure that personal information used to make a decision that affects an individual is accurate and complete.

#### **What is required?**

- A public body must have procedures in place that ensure that the accuracy and completeness of personal information is appropriate for the purpose for which the personal information is used. Some procedures that may assist are:
  - verifying the identity of an individual from whom personal information is collected (especially important when personal information is collected by telephone or electronically);
  - using validation processes for data within electronic systems;
  - providing for regular updating, if necessary, and recording when personal information in a record was last updated;
  - using the most reliable sources to update personal information and recording the source of the information;
  - allowing individuals to review their own personal information and request correction or annotation in case of errors or omissions.

### **Correction of personal information**

**Section 36** **Section 36** requires a public body to respond to requests for correction of personal information and to notify other public bodies, or third parties to which the information has been disclosed, about the request and about any correction or annotation that was made in response to the request.

#### **What is required?**

- Procedures must be in place to ensure that a public body can respond to a request by an individual for access to his or her own personal information and to a request for correction of that information. It should not normally be necessary for an individual to make an access request under the *FOIP Act* before requesting a correction of personal information.



- Procedures must in place so that notification of a correction or annotation of personal information can, if necessary, be sent to any other public body or third party to which the information has been disclosed during a one-year period prior to the request for the correction or annotation.
- A record of purpose must be maintained for any use or disclosure of personal information that is not included in the public body's Directory of Personal Information Banks. The record of the purpose for the disclosure must be either attached or linked to the personal information (**section 87.1(3)**).

### **Directories of personal information banks**

**Section 87.1** The head of a public body is responsible for maintaining and publishing a directory of its personal information banks, either in printed or electronic form. The directory of personal information banks must include

- the title and location of the personal information bank;
- a description of the kind of personal information and the categories of individuals whose personal information is included;
- the authority for collecting the personal information in the bank; and
- the purposes for which the personal information is collected or compiled and the purposes for which it is used or disclosed.

#### **What is required?**

- A public body must publish a directory of personal information banks that includes the elements listed in **section 87.1(2)**. The description of the personal information and the statement regarding the purposes for which the information is used or disclosed must provide sufficient detail to be meaningful to individuals whose information may be included in the personal information bank.
- The directory must be kept as current as is practicable, and access to the directory made available to the public at an office of the public body (**section 87.1(4)**).
- Each time personal information is used or disclosed for a purpose that is not included in the directory, a record of the new purpose must be kept and the record of that new purpose must be either attached or linked to the personal information (**section 87.1(3)(a)**).
- The new purpose(s) must be included in the next publication of the directory (**section 87.1(3)(b)**).

#### **For consideration**

The Act establishes minimum requirements for the directory. Public bodies may wish to consider including additional information, such as a list of the public body's information-sharing agreements and information about retention periods.

### **Retention of personal information**

**Section 35(b)** **Section 35(b)** requires retention of personal information used to make a decision about an individual for one year from the date of last use in most cases.

**What is required?**

- Personal information must be retained for a least one year after it is used to make a decision affecting an individual (including a decision relating to a request under the *FOIP Act*). This requirement overrides any retention period in a public body's records retention and disposition schedule. For example, personal information used by a public body to determine an individual's eligibility for a program or service must be retained for one year after it is used, even if the public body's records retention schedule would normally require the information to be disposed of at an earlier date. The one-year period gives individuals an opportunity to request access to personal information used to make the decision, to ensure that it is accurate.
- If personal information is retained for a shorter period of time, there must be an agreement to that effect in writing between the individual, the public body and the body that approves the records retention and disposition schedule.

**For consideration**

- Records retention and disposition schedules should be in place for information in personal information banks and for the administrative or electronic systems in which they operate.

**Protection of personal information**

**Section 38** A public body must make reasonable security arrangements for the protection of personal information against such risks as unauthorized access, collection, use, disclosure, and destruction. The basic attributes for a comprehensive security policy and practices are provided in section 9.5 of this chapter.

**What is required?**

A public body must have safeguards in place that are appropriate under the specific circumstances. The type and level of security measures will depend upon a range of factors, most importantly, the sensitivity of the personal information. The following are guidelines; these security arrangements may not be required in all circumstances.

- A public body should have a written security policy and procedures governing operations that involve personal information.
- There should be a responsible official who has authority for information security.
- There should be documented procedures for collecting, processing, accessing, transmitting, storing, and disposing of personal information.
- Security procedures should cover administrative, physical and technological security, including
  - a threat and risk management methodology;
  - a process for designating sensitive information;
  - a system of authorization and access procedures (e.g. identification cards, keys, codes, combinations, badges and system passwords), and the maintenance of control records for gaining access to sensitive personal information;

- controls over authorization to add, change and delete personal information in an electronic information system, and audit capacity;
  - procedures to ensure that qualified personnel are involved in the maintenance of electronic systems in order to ensure configuration control of equipment, systems, networks, and the updating of operating procedures;
  - procedures for ensuring communications security;
  - procedures for personnel screening that are commensurate with the sensitivity of the personal information involved;
  - controls that restrict use of personal information to the purposes for which the information has been collected and restrict access to those officials and employees who have a “need to know” the information (i.e. access is limited to the specific portions of the personal information needed for the function being performed);
  - appropriate physical security measures, such as security access zones, locked rooms, storage cabinets, controlled positioning and access to computer terminals and faxes (to prevent random access), as well as checkout and secure transmission procedures for files;
  - technological security measures appropriate to the nature of the personal information stored on a device and the type of device used (e.g. encryption and password protection for portable data devices); and
  - secure disposal procedures for records and equipment commensurate with the level of sensitivity of the personal information and its vulnerability to compromise.
- There should be procedures for monitoring and reviewing the general effectiveness of security measures, including those relating to the protection of personal information.
  - There should be written sanctions or consequences for contravention of security procedures and policies.

### Use

*Section 39* **Section 39** limits the purposes for which public bodies may use personal information.

#### *What is required?*

- The personal information in a system or program must be used only
  - for the purpose for which it was collected or for a use consistent with that purpose,
  - with the consent of the individual; the form of consent must be in accordance with **section 7** of the FOIP Regulation,
  - for a purpose for which information may be disclosed under **section 40, 42 or 43** of the Act, or
  - in the case of personal information in the alumni records of post-secondary educational bodies, for the purposes of their own fund-raising activities; this use must be discontinued at the request of an individual whose personal information is being used in this way.

- The amount and type of personal information used must be limited to what is necessary for the public body to carry out its purpose in a reasonable manner.

### **Disclosure**

**Section 40** A public body may disclose personal information only in accordance with the provisions of **section 40**.

#### ***What is required?***

- Any disclosure must be permitted by one of the provisions of **section 40(1)**, **section 40(2)** or **section 40(3)** of the Act.
- The amount and type of personal information disclosed must be limited to what is necessary for the public body to carry out its purpose in a reasonable manner.
- If disclosure is not permitted under **section 40(1)**, **(2)** or **(3)** of the Act, persons or bodies outside the organizational unit that operates and uses the system or program must not have access to information in the system, program or personal information bank, either directly through electronic means or through receipt of hard copy, tapes, disks or other copies.

### **Research or statistical purposes**

**Section 42** A public body may disclose personal information for a research purpose only under specified conditions.

#### ***What is required?***

- Access to personal information in individually identifiable form must be necessary to reasonably accomplish the purpose of the research, or the Information and Privacy Commissioner must have approved the research purpose.
- Any record linkage must not be harmful to the individuals the information is about.
- The benefits of the record linkage must clearly be the public interest.
- The researcher must have signed an agreement to comply with security and confidentiality conditions, to meet a schedule for the destruction of individual identifiers and to ensure that there is no subsequent use or disclosure of the information in individually identifiable form without express authorization.
- The agreement must meet the requirements set out in **section 9** of the FOIP Regulation.

All of the above requirements must be in place before personal information may be disclosed under **section 42**.

### **Data sharing and data matching**

Data sharing and data matching involve the disclosure or comparison of personal information for an authorized purpose. These activities may involve public bodies only or public bodies and other organizations. The data sharing or matching may

occur through electronic or other forms of transmission and may consist of single transactions or programs that continue over a period of time. These activities are subject to the provisions of **Part 2** of the *FOIP Act*.

See section 9.7 of this chapter for definitions and a detailed discussion of data sharing and data matching. Also, see the *Guide for Developing Personal Information Sharing Agreements*, published by Access and Privacy, Service Alberta.

#### **What is required?**

- In any data sharing or data matching,
  - there must first be authority to collect the information under **section 33** and to collect information indirectly under **section 34**;
  - the uses must meet the requirements of **section 39**;
  - if a disclosure is for research purposes, the requirements of **section 42** or **43** must have been met.

If the above requirements are not met, the data sharing or matching may not be in compliance with **Part 2** of the *FOIP Act* and the public body must modify or discontinue this activity.

#### **For consideration**

- Consider notifying the individuals whose personal information may be the subject of data sharing or data matching at the time the information is collected.

## 9.2 Privacy Considerations when Planning New Programs, Administrative Practices or Information Systems



**Public bodies should establish practices and procedures that take into consideration the requirements of Part 2 of the Act in the planning, design, development of specifications, and implementation of new or modified personal information systems, programs, administrative practices or legislation.**

To ensure that privacy protection requirements, as set out in **Part 2** of the *FOIP Act*, are taken into account in the application of new technologies, or when an administrative practice or program is being developed or modified, public bodies may need to conduct a privacy impact assessment and submit it to the Information and Privacy Commissioner for review. The program official responsible for developing or implementing the new technology, administrative practice or program should develop a privacy impact assessment, as part of a development team that could include IT specialists, the FOIP Coordinator, the records manager, etc. The privacy impact assessment would be developed as part of the business needs analysis or project initiation stage of the project. See section 9.3 of this chapter for detailed information on how and when to conduct a privacy impact assessment and who to involve in its development.

Privacy and security measures should not be viewed as barriers to applying innovative technology. Rather, they are essential components of modern systems that serve to build public confidence in the use of technology. In the last decade, a number



of technologies have been specifically developed to be privacy-enhancing technologies. Technologies such as encryption, digital signatures, anonymous electronic cash and service delivery systems, and “pseudo-identification” can often enhance privacy at little or no extra cost to the program. These technologies may also have the advantage of providing more secure identification to reduce fraud, more secure networking to reduce losses from theft, and more secure payment systems to eliminate the administrative costs of cash transactions.

Systems development should take into consideration the privacy rights of individuals and the protection of personal information. This applies to all aspects of the management of information, including collection or compilation, controls on accuracy, use and disclosure, protection, and disposal. Privacy considerations should be integrated at the earliest stages of development of automated information systems to ensure that such systems meet legal and policy requirements.

---

### 9.3 Privacy Impact Assessments

A *privacy impact assessment* (PIA) is a process that assists public bodies in reviewing the impact that a new program, administrative process or practice, information system or legislation may have on individual privacy. The process is designed to ensure that the public body evaluates the project or initiative for technical compliance with the *FOIP Act* and also assesses the broader privacy implications for individuals. A PIA is both a due diligence exercise and a risk management tool. Although only real breaches of privacy contravene the privacy provisions of the *FOIP Act*, even the perception that privacy may not be adequately protected can seriously damage the reputation of a public body, as well as the public’s confidence in a particular program or initiative.

The PIA process requires a thorough analysis of the potential impact of the initiative on privacy and a consideration of measures to mitigate or eliminate any negative impact. The PIA is an exercise in which the public body identifies and addresses privacy risks that may arise in the course of its operations. While PIAs are focused on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy and security policies and procedures, or the lack of them, can be significant factors in the ability of the public body to ensure that privacy protection measures are available for specific projects.

A PIA provides documented assurance to the public body, to the Information and Privacy Commissioner and to the public that all privacy issues related to the initiative have been appropriately identified and addressed. Once the Office of the Information and Privacy Commissioner is satisfied that the public body has addressed the relevant considerations and is committed to the provision of the necessary level of privacy protection, the Commissioner or a staff member will accept the PIA. Acceptance is not approval. It merely reflects that Office’s acceptance that the organization has made reasonable efforts to protect privacy.

#### **When is a privacy impact assessment needed?**

Public bodies that are custodians and therefore subject to the *Health Information Act* for health information in their custody or under their control, should note that there

are express requirements under the *Health Information Act* to conduct privacy impact assessments in certain situations. Some of the public bodies under the *FOIP Act* that are affected by those requirements are the Alberta Health Services Board and the department and Minister of Alberta Health and Wellness.

Privacy impact assessments are not mandatory under the *FOIP Act* but are recommended for major projects that involve the collection, use or disclosure of personal information. **Section 53(1)(f)** of the *FOIP Act* provides authority for the Commissioner to comment on the implications for freedom of information or for protection of privacy of proposed legislative schemes or programs of public bodies.

Public bodies should consider conducting a PIA when

- new data elements will be collected and added to an existing personal information database, or a new database is proposed;
- system access will be rolled out beyond current parameters, controls, levels or numbers of users;
- the use of personal information will be expanded to include data linkage or matching or other purposes;
- limited disclosure or reporting about selected individuals will be expanded to enable broad disclosure of information about a larger population base;
- the way in which the system is accessed, managed or secured from a technical or managerial perspective is changed significantly (e.g. use of internet technology);
- initiatives involving multiple public and/or private sector bodies that result in the compilation of personal information;
- management or security of the system is outsourced; or
- the retention period for personal information in the system will be changed.

As information systems become more complex, the probability of having an unexpected impact on privacy increases. Initiatives that appear to involve minor technical enhancements for client convenience and public body efficiency may significantly impact individual privacy.

The Office of the Corporate Chief Information Officer, Government of Alberta, is responsible for ensuring that government information and communications technology (ICT) projects, especially cross-government projects, comply with all applicable privacy legislation. The Office coordinates policy development, privacy impact assessment procedures and privacy architecture development for ICT in the Government of Alberta.

### **What is the process for a PIA?**

#### ***Consider establishing a PIA development team***

Determine which staff can best provide the information that is needed for the PIA. The team could include the FOIP Coordinator, the project or program sponsor, records manager, project manager, IT specialists, legal services, communications specialist and a senior or executive manager.

Identify someone to lead the process and write the PIA. Ideally, this would be someone who understands the *FOIP Act* and privacy principles and issues, has technical writing skills, has project management experience and can synthesize input from a variety of sources.

***Consider when to start the process***

If the PIA is viewed as an obstacle to the initiative being launched, it has been started too late. If decisions about the initiative are not firm, resources have not been committed and questions about privacy implications cannot be answered, it is too early to start the process.

According to the Office of the Information and Privacy Commissioner, the PIA is a dynamic document that should be updated from time to time as changes are contemplated for the program; it is rarely ever finished. Public bodies are expected to advise the Commissioner's Office of any changes or modifications to the program and to provide documentation so that the PIA on file is always up to date.

If the project is complex, a cross-government initiative, or involves a high volume of personal information, consider consulting with Access and Privacy, Service Alberta to provide input on project design.

***Determine who will approve the PIA internally***

The internal approval of a PIA should be based on the public body's established internal approval process and should include approval from the members of the PIA development team.

***Consider whether public consultation is needed***

It may be appropriate to consult with stakeholders or the broader public on major initiatives or on significant overhauls of existing programs. Focused public discussion conducted early in the process can help program or system designers anticipate public reaction to proposals or help to eliminate options that meet with significant resistance. The public body should address in the PIA how it intends to educate and consult with affected stakeholders respecting the proposed initiative. Alternatively, the justification for not consulting should be set out in the PIA.

***Understand the role of the Office of the Information and Privacy Commissioner***

To give the Commissioner's Office time to formally review and comment, public bodies should provide the PIA to the Office at least 45 working days before implementing the proposed new or changed practice or system. In practice, however, the role of the Commissioner's Office starts long before the formal review. The process for interaction with the Commissioner's Office is as follows:

- The public body (usually the FOIP Coordinator) advises the Commissioner's Office of the project well in advance of implementation.
- If necessary, the PIA development team meets with the staff of the Commissioner's Office to review the project and determine whether a PIA is required. The Commissioner's Office decides whether a PIA is advised and requests the public body to conduct one.

- If a PIA is required, it must be submitted to the Commissioner by the head of the public body.
- The PIA development team prepares the PIA by completing the PIA Questionnaire (published by the Office of the Information and Privacy Commissioner), with the necessary elaboration and enclosures and submits it (through the head) to the Commissioner. The FOIP Coordinator may send a working copy of the document to the staff of the Commissioner's Office prior to the head's submission.
- Questionnaire responses are reviewed by the Commissioner's Office and discussed with the PIA development team or its leader, as required. Further information may be requested, which could result in an extension to the optimal 30-day review period.
- Upon final acceptance by the Commissioner's Office, the head of the public body receives a letter of acceptance from the Commissioner.
- The PIA is filed in the library of the Commissioner's Office and is available for public review. Public access to some confidential information, such as details of sensitive security measures, is sometimes restricted. Any such restrictions are limited and specific.
- The public body provides updates to the PIA as changes to the project are implemented over time.

The Commissioner's Office may use the PIA as a starting point for any investigation into a breach of privacy.

The Office of the Information and Privacy Commissioner publishes a document on the PIA process called *Privacy Impact Assessment: Instructions and Annotated Questionnaire*. The Office also publishes a *Privacy Impact Assessment: Supplementary Organization Questionnaire* that is intended for use in projects involving more than one organization. These packages are available from the Commissioner's website at [www.oipc.ab.ca](http://www.oipc.ab.ca), or by requesting a PIA package by contacting the Office (780-422-6860; or toll free 1-888-878-4044).

### **Privacy impact assessment questionnaire**

The PIA Questionnaire will be considered a public document by the Office of the Information and Privacy Commissioner. Any appendices or attachments will also be considered public documents unless they are explicitly designated as confidential. Examples of appendices would be an organizational strategic or business plan addressing privacy protection or physical or information security plans and access control documentation. Appendices that are designated as confidential must be accompanied by the reasons for the confidentiality.

The PIA Questionnaire must be submitted to the Commissioner with a covering letter from the head of the public body in order to receive a formal response.

For public bodies that are also custodians under the *Health Information Act*, there are statutory requirements for privacy impact assessments in sections 46, 64, 70, and 71 of that Act that must be complied with. Those bodies may use the same PIA

Questionnaire for conducting a PIA under the *Health Information Act* with a few modifications. (For more information on conducting PIAs for purposes of the *Health Information Act*, see Chapter 5, section 5.2.7 of the *Health Information Act Guidelines and Practices Manual*, published by Alberta Health and Wellness.)

The questionnaire is divided into two parts:

- Part A: Organizational Privacy Management; and
- Part B: Project Privacy Management.

Each part contains a series of questions. The checkboxes on the questionnaire provide for summary responses to the questions. The note fields provide for elaboration of the responses, as necessary. There is also a column that can be used to cross-reference separate enclosures. The questionnaire can be completed either in paper or electronic formats.

#### **Part A: Organizational Privacy Management**

This part of the questionnaire is intended to provide background on facets of privacy management across the public body which may affect the management of privacy issues for the specific project. If this information has been provided with a previous PIA and has not changed, it does not have to be resubmitted. One set of questions in Part A is designed to provide information, including documentation if available, from the public body about its privacy protection policies, controls and procedures. This would include such things as a privacy charter, policy or strategic plans relating to privacy protection and any procedures that have been developed with respect to information security, records management, disposition processes, need to know, etc.

The second set of questions deals with the structure and organization for dealing with security and privacy protection within the public body. This would include information on whether a position in the organization has been designated as responsible for privacy and security; the management reporting process for dealing with privacy compliance issues and training of new staff in privacy protection.

#### **Part B: Project Privacy Management**

In this part of the questionnaire, the public body provides information specific to the proposed project. The information requested includes

- a project description, including a listing of data elements to be collected, used or disclosed; an information flow diagram; and a listing of who will have access to the information;
- an analysis of the proposed information flows in relation to the rules in the governing privacy or other legislation regarding collection, use, disclosure, protection, accuracy, retention and disposition of personal information;
- a privacy risk assessment in which the public body identifies the privacy risks of the project and shows whether those risks have been successfully addressed through system design or policy measures or through other proposed options for mitigation. The residual risks that cannot be addressed through the proposed options should also be identified. Where possible, the likely implications of those risks in terms of public reaction and project success should be analyzed;



- a description and relevant documentation related to the privacy controls and security measures or procedures for the specific project; and
- the arrangements that have been made for audit, compliance and enforcement mechanisms for the proposed project, including information about how audits would be conducted and how any identified privacy issues would be addressed.



**When the development of personal information systems is contracted out, the need to develop privacy impact assessments should be among the privacy requirements included in any management or operations contract governing the project and should be identified in the Request for Proposals or Tender documentation.**

For more information, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

#### 9.4 Reviewing Forms and Other Collection Instruments

**Section 34(2)** of the *FOIP Act* establishes a notification requirement for public bodies when collecting personal information. Public bodies must notify individuals whose information is being collected of the purpose for which personal information is being collected, the legal authority for the collection, and the title, business address and business telephone number of someone who can answer questions about the collection.

Forms are a common way of collecting personal information, so it is particularly important to ensure that paper and electronic forms comply with the requirements respecting collection and notification in **sections 33 and 34** of the Act. Compliance with these requirements

- supports the right of individuals to know what personal information public bodies collect about them and how this information is used;
- supports the right of individuals to access information about themselves; and
- helps maintain confidence among individuals that public bodies are protecting their personal information from unauthorized collection, use and disclosure.

As indicated in sections 7.1 and 7.2 of Chapter 7, ensuring compliance with **sections 33 and 34** of the Act requires ongoing review of a public body's collection activities. This review should include an assessment of all new forms used to collect information directly from individuals to ensure that the forms comply with the Act and that the public body is not collecting personal information without the legal authority to do so.

In cases where some personal information on a form should no longer be collected, public bodies should inform staff and clients that certain fields must not be filled out or staff should cross them out, where possible. These instructions should be provided in writing to staff. In some instances, it may be possible to black out fields that are no longer required.

A review of the collection of personal information should cover all collection instruments, including survey questionnaires in print or electronic form. For information on privacy protection when conducting surveys, see *Conducting Surveys: A Guide to Privacy Protection*, published by Access and Privacy, Service Alberta.

A review should also consider collection of personal information through the public body's website, and particularly in forms submitted from websites. For further information on developing privacy statements for websites, see the *Guide to Developing Privacy Statements for Government of Alberta Web Sites*, published by Access and Privacy, Service Alberta.

A review of forms and other collection instruments may be combined with the privacy compliance review, discussed in section 9.1 of this chapter.

### **Notification**

The notification (collection notice) may be printed on the collection form itself, on a separate or covering document that explains the form and how to fill it out, or it may be given orally. Oral notification is practical when information is taken personally over the telephone or taken during an interview.

When the collection notice is provided orally, the individual may be provided with a copy of the notice, either at the office where collection takes place or with the documentation sent to an individual to confirm collection of information over the telephone or electronically.

An example of notification is as follows.

*This personal information is being collected under the authority of [state Act or program mandate] and will be used to [state all of the known purposes]. It will be treated in accordance with the privacy protection provisions of **Part 2** of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection, contact [position, address, and business telephone number of responsible official or employee].*

### **Optional practices**

There are a number of practices for the collection of personal information through forms that reflect good management of personal information but are not mandatory under the *FOIP Act*.

Here are some best practices.

- Design forms to ensure that the individual from whom the information is collected is given a copy of the notification and that a copy of the notification is also retained by the public body;
- Design forms to place the collection notice either at the top of the form (before any personal information is collected) or just above the signature line, where practicable;
- Provide detailed notifications, where appropriate, to inform the individual about his or her right to request correction of inaccurate or incomplete information, the

right to appeal refusals of corrections and the role of the Information and Privacy Commissioner in reviewing such refusals;

- In consultation with the FOIP Coordinator or FOIP Office, conduct a central review of all new forms and proposed revisions before finalization for printing, including review of privacy issues; and
- Where personal information is collected from a source *other than the individual the information is about* (indirect collection), include provisions to inform individuals generally that information about them is being sought from a variety of specific sources. Such explanations should be included in documentation or brochures given to individuals who are the subjects of the indirect collection. They are also required in your personal information bank description. Notifying individuals about indirect collection may not be possible or practical in cases where the personal information collected is about the spouse, dependent or emergency contact of an applicant.

### Collecting information on-line

When collection of personal information takes place in an electronic environment, public bodies should have the capacity to audit the public body's authority to collect the personal information, its manner of collection and its notification of collection and use. The following practices or other comparable audit practices should be in place.

- Establish a policy and accountability structure to ensure that electronic forms, which are often generated on a decentralized basis, include notification;
- When new forms software is under consideration, consider whether it permits the easy addition of notices in ways that are convenient and that effectively inform the individual filling out the electronic form of his or her privacy rights;
- Provision should be made for authorization of indirect collection and for authorization of additional uses or disclosures of the information on electronic forms where this is appropriate, as well as for a signature or other verification of the identity of the individual providing the authorization;
- If necessary and practicable, a hard copy of the form should be provided to the individual the information is about, including the collection notice on the form; and
- The public body should be able to retain a copy of the notice and authorization, if applicable.

## 9.5 Developing a Security Policy

**Section 38** of the Act requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

*Reasonable security arrangements* are usually practices and procedures expressed through a security policy approved for use within a public body. This policy should be based on a threat and risk assessment of the information and assets in the custody or under the control of a public body, and include physical, administrative and technological security.

Public bodies that are also custodians under the *Health Information Act* must comply with section 60 of the *Health Information Act* and section 8 of the *Health Information Regulation* in order to ensure that the privacy of individuals and the confidentiality of their health information is protected. For more information about developing a health information security policy, see Chapter 11, section 11.3.4 of the *Health Information Act Guidelines and Practices Manual*, published by Alberta Health and Wellness.

Government of Alberta departments should refer to the *Information Technology Security Policy* and the *Policy for the Transmission of Personal Information Via Electronic Mail and Facsimile*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta.

The Office of the Information and Privacy Commissioner has also produced a document entitled *Information Security Plan*, which is Appendix 1 to the *Privacy Impact Assessment: Instructions and Annotated Questionnaire*, produced by that Office. In its *Security Plan*, the Office of the Information and Privacy Commissioner recommends that the following policies outlining end-user responsibilities relative to the computing environment be developed:

- computer usage policy and guidelines;
- e-mail policy and guidelines; and
- internet policy and guidelines.

Government of Alberta departments and agencies should refer to the *Internet and E-mail Use Policy*, available on the Corporate Human Resources website, and *Managing Electronic Mail in the Government of Alberta*, published by Records and Information Management, Service Alberta. Public bodies should also consider policies related to the use of wireless technology.

### **Basic attributes of a comprehensive security policy**

Many organizations have security policies that apply to specific security issues, such as access to classified information, administrative security or information technology security. A more comprehensive approach to security administration, including all aspects of physical, administrative and technological security, is both necessary and practical.

The sharing and use of personal information by a number of public bodies creates an additional challenge. The Act requires reasonable protective measures for such information, but this will now require more consistency among public bodies in how they handle and protect such information. Being able to compare protective measures among public bodies doing public business with each other is essential.

### **Authority**

A security policy should contain a statement of the authority or authorities under which the security policy is being issued and a direction from the senior officer of the public body on its effective implementation.

**What needs to be safeguarded**

All assets of a public body, including information, require good basic care. Some assets, however, are more sensitive or valuable and require additional safeguards. A security policy should include a requirement to carefully identify sensitive information, valuable assets and information systems that may need additional safeguards.

**Sensitive information**

Certain information must be withheld from access under the *FOIP Act* because it would reveal particular sensitive information or pose possible injury to public or private interests. These categories of information are described in the exceptions to access in **sections 16 to 28** of the Act. Public bodies should take greater care in protecting these categories of information than they would information that is generally available to the public.

Among these categories is personal information. The Act defines personal information in **section 1(n)**, and **section 17** provides guidance as to what may be an unreasonable invasion of personal privacy. **Section 17** is considered in detail in section 4.3 of Chapter 4 of this publication. The categories in **section 17** help to identify sensitive personal information that may need safeguards. Health information, financial information, pay and benefits information, and criminal records are particularly sensitive and require special protection.

**Threat and risk assessments**

The security policy should require a threat and risk assessment to be conducted. This should include identification of what information is likely to require safeguards and an assessment of threats and risks to the information and information systems. This analysis provides the basis for assigning safeguards at a level commensurate with the risk. The security measures can be monitored and adjusted over time. To assist in the threat and risk assessment process, the security policy should

- require program areas to maintain complete and up-to-date inventories of personal information and personal information systems; and
- provide for the review of potential threats (e.g. how could sensitive personal information be lost or changed?, what impact would this have on client confidence in the programs?, who would be affected and how?).

The Government of Alberta's *Information Technology Security Policy* requires all information systems to be given a risk classification (scaled from no-risk to critical applications) depending upon the nature and use of the system. Critical applications need to be included in business continuity plans and to have the most stringent security mechanisms in place for protection.

See section 9.6 of this chapter for more detailed information on conducting threat and risk assessments.



### ***Types of safeguards***

***Administrative safeguards.*** Examples of administrative safeguards include:

- designating a position that has overall responsibility for security within the public body;
- ensuring that staff understand their responsibilities and the public body's security procedures by providing them with written procedures and instituting training programs;
- arranging to resume operations in the case of loss of computer-based data or capabilities;
- checking the references and background of an officer or employee to ensure that he or she is a suitable person to have access to sensitive information, information systems and the facilities where they are located;
- implementing the "need-to-know" principle where access to particular information or systems can be limited to certain officers and employees who have a need for such access because it is necessary to perform their duties;
- conducting process audits and periodically reviewing access logs, etc.; and
- establishing sanctions for breaches of the security policy and a process for reporting and investigating breaches.

***Physical safeguards.*** Examples of physical safeguards include:

- periodic reviews of physical security features, such as alarms, fences, and codes for cipher locks;
- use of physical barriers, security zones, access and authorization mechanisms, and locked containers to restrict access;
- use of proper containers and procedures for the secure processing, storage, transmission and disposal of information and other assets;
- specifying adequate fire and fire safety procedures; and
- designating off-site storage facilities with a similar level of physical and environmental security.

***Technological safeguards.*** The security of computer and telecommunications equipment and systems requires special consideration. This is partly because of the need to protect sensitive information, such as certain categories of personal information, and because of the significant extent to which many public body operations and services are dependent on information technology.

In addition to protecting the confidentiality of the information in these systems, it is necessary to protect the integrity and availability of a public body's information technology systems. Defining the importance of the availability of information and services is the first step in making plans to resume business within acceptable time and resource limits in the event of loss of data, programs or systems.

Also important is the identification of potentially vulnerable communications systems. The risk of someone overhearing sensitive personal information on the telephone or through a data line should not be neglected, given the ease of such

access. Facsimile machines warrant special attention because of the chance of misdirecting sensitive information through an error in transmission and because they are generally accessible to anyone in an office area.

Examples of technological safeguards include:

- using software, hardware or operating system access controls such as passwords, termination on inactivity, clearance of display screens, transaction logs and error logs;
- using secure communications and encryption, especially for mobile devices such as laptops;
- providing adequate virus protection for new and existing computer equipment;
- establishing security controls for remote access to information systems;
- restricting the use of less secure forms of communications (e.g. cellular telephones); and
- conducting audit checks of data and system integrity, and establishing procedures for database recovery and back-up.

#### ***Breaches, sanctions and review***

A security policy should establish what are considered to be breaches of security and should require that all breaches be reported to the chief officer of the public body.

A security breach is an unauthorized access to or collection, use, disclosure or disposition of personal information. A breach may be accidental or intentional.

The security policy should state how an investigation into a breach of security would be conducted. The policy should also set out any administrative or disciplinary sanctions that will be applied if a breach is found. Sanctions may consist of the removal of access to sensitive information or information systems, verbal or written reprimand, suspension without pay, or dismissal. The sanction will depend on the policies of the public body, the circumstances and the record of the officer or employee.

**Sections 92(1) and 92(2)** of the *FOIP Act* provide that a person must not collect, use or disclose personal information, or attempt to gain or gain access to personal information in contravention of the Act. A person who does so is guilty of an offence and liable of a fine up to \$10,000 (see sections 2.10 and 2.11 of Chapter 2 of this publication for a further discussion of liability, offences and penalties).

A security policy should ensure a fair and equitable process for dealing with individuals who have consented to personnel security checks or are subject to disciplinary action related to security. A clear process for appeal and review should be put in place.

#### ***Security in contracting***

Protective arrangements under **Part 2** of the Act apply to personal information in the custody or under the control of public bodies. This may include information that is collected, compiled, used, disclosed or disposed of by a contractor. A security policy should state that its provisions apply to persons working under contract to a public

body when they are required to handle sensitive personal information or have access to information systems or facilities where such information is handled or stored. The physical, technological and administrative security requirements for individual contracts will have to be decided on a case-by-case basis.

A security policy should also include a process for determining the conditions under which the processing or storage of personal information can be outsourced. Special consideration should be given where the personal information is sensitive in nature, or where the contractor is located outside Alberta or Canada.

For information on establishing security and other requirements during the contracting process, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta, and *Public-Sector Outsourcing and Risks to Privacy*, from the Office of the Information and Privacy Commissioner.

---

**9.6**  
**Conducting**  
**Threat and Risk**  
**Assessments**

While no system, including an information technology system, can be made absolutely secure, it is possible to manage the impact of threats to business processes and to individual privacy. This is done through development of security management processes to reduce, transfer, avoid or accept risks. The senior management of a public body must find an appropriate balance between the potential threats and risks and the cost of protection. To properly identify those risks, threat and risk assessments should be undertaken for the personal and other sensitive or confidential information in the custody or under the control of a public body.

In Government of Alberta departments, Chief Information Officers are responsible for initiating appropriate threat and risk assessments prior to the approval of design specifications for new information systems, whenever a significant change occurs to the systems, or on a yearly basis. If a new system or program or an enhancement to an existing system or program deals with the collection, use or disclosure of personal information, a privacy impact assessment may be necessary (or required, for public bodies that are also custodians under the *Health Information Act*). In other public bodies, the person responsible for information security could adopt the same approach as that of government departments regarding when threat and risk assessments should be initiated.

The threat and risk assessment process should be flexible enough to be able to recognize new risks as they arise. Current threats may need to be re-evaluated and potential or anticipated threats identified as the nature of the information in the custody or under the control of a public body changes.

For information regarding the development of a comprehensive security policy, see section 9.5 of this chapter.

**Components of a threat and risk assessment**

***Determine what needs to be protected and what level of protection is required***

Information in the custody or under the control of a public body should be grouped according to the function, process, program or service it supports. Within each group, determine the requirements that the information may have for its protection. All the

data elements or information, software, users, administrators, analysts, storage facilities, storage media, system documentation, etc. should be listed.

***Define the threats to protect against***

For each grouping of personal or other sensitive information,

- identify the potential agents or events that could place the information at risk (e.g. theft, unauthorized access, viruses, power loss, etc.);
- classify each agent or event by the type of threat;
- determine the likelihood that the event may occur; and
- identify the potential consequences and rate the impact of the event if it were to occur.

Threats to the security of information may be

- *a threat to the confidentiality of information*, where information is made available or disclosed to unauthorized individuals, entities or processes;
- *a threat to the integrity of information*, where data and information technology systems are altered or destroyed from their intended form in an unintentional or unauthorized manner; and
- *a threat to availability of information*, where information is not consistently retrievable to enable public bodies to meet their business and legal obligations (e.g. under the *FOIP Act's* access to information provisions).

Some examples of these threats are:

- unauthorized access to a database as a result of an error in the way access controls have been configured – this may affect the confidentiality, integrity and availability of information;
- malicious code being inserted by a disgruntled or misguided employee into a network – this may affect the confidentiality, integrity and availability of information;
- unauthorized access to a database as a result of password interception, cracking or network/operating system vulnerability – this may affect the confidentiality, integrity and availability of the information;
- unauthorized access to information as a result of verbal disclosure by an employee, leaving information where it can be viewed by unauthorized persons, electronic interception of information from a fax line or cellular phone, faxing or e-mailing information to the wrong fax number or e-mail address.
- access by an unauthorized individual to information stored on an employee's or contractor's home or laptop computer – any of these occurrences may affect the confidentiality and integrity of the information;
- service interruption as a result of a power failure, labour dispute, or denial of service attack on an Internet server or provider – this may affect the availability of information;

- accidental or deliberate loss of data as a result of physical damage to hardware, wilful destruction of recorded information, information destroyed in a flood or fire – this may affect the availability of information;
- removal of equipment, such as theft of a laptop or file containing sensitive information – this may affect the confidentiality, integrity and availability of information; and
- records being misdirected or misfiled, or destroyed in a manner that is not in accordance with approved records retention and disposition schedules or policies – this may affect the confidentiality and availability of information.

***Estimate the likelihood of the threat scenario occurring and the potential impact or injury that could result***

Public bodies should determine the likelihood (low, medium or high) of each or any of the above threats occurring. Then, the potential consequences of the events need to be identified and their seriousness rated. Some of the potential harms would be

- litigation;
- loss of trust by clients;
- loss or delay of service;
- loss of confidentiality;
- cost of notifying affected individuals; and
- cost of system repair.

***Assess whether current or proposed security measures are appropriate to reduce the risk***

Given the potential threats to the information that have been identified and the likelihood and impact of an event occurring that would place each group of personal or other sensitive information at risk, public bodies should assess the adequacy of existing safeguards and current resources to protect against those potential threats.

This assessment involves listing the existing safeguards that protect against the threat or event, considering whether the information might still be vulnerable and rating the risk. A low risk will require some attention and consideration for safeguard implementation. Moderate risk requires attention and safeguard implementation in the near future. A high risk requires immediate attention and immediate safeguard implementation.

***Identify how to manage the residual risk after implementing safeguards***

Identify any additional safeguards recommended to lower the risk to an acceptable level and describe the proposed measures or safeguards. Different safeguards provide different levels of protection. Selection of the most appropriate safeguard will depend upon the availability of resources and the acceptable level of risk. Implementing some safeguards to lower the projected risk level may, in some cases, not be practical because of technical or physical limitations or because of time or financial constraints.



## 9.7

Privacy  
Considerations  
for Data Sharing  
and Data  
Matching**Data sharing**

*Data sharing* refers to one public body collecting information from or disclosing information to another public body or other organization for such purposes as

- determining or verifying the eligibility of a client for a program, benefit or service;
- detecting duplicate payment of benefits from two public bodies;
- determining an individual's suitability for an honour or award; and
- delivering a joint program.

There are no specific controls over data sharing in **Part 2** of the *FOIP Act*. However, the collection, use and disclosure provisions of the Act govern how such activities can be carried out and the Information and Privacy Commissioner may comment on the privacy implications of the proposed data sharing (**section 53(1)(g)**).



**When a public body determines that sharing some of the personal information it holds is necessary, and the sharing is authorized under the disclosure provisions of the *FOIP Act*, this should be supported by a written personal information sharing agreement.**

Using a personal information sharing agreement to establish the terms and conditions that will apply to a transfer of personal information has the benefit of

- providing a formal mechanism for the efficient and timely sharing of personal information;
- limiting the type and amount of personal information that will be disclosed and the purposes for which it will be used; and
- providing additional privacy protection, both during and after the sharing, by binding the parties to enforceable terms and conditions.

For further information on data sharing, including the components of a personal information sharing agreement, see the *Guide to Developing Personal Information Sharing Agreements*, published by Access and Privacy, Service Alberta.

**Data matching**

*Data matching* means the comparison (often by computer) of one or more databases or sets of records of personal information held by one public body or organization with one or more other databases or sets of records held by a different public body or organization, where the computer matching program creates or merges files on identifiable individuals, and where the matched data is used to make decisions about the individuals to whom the data relates. Data matching tends to involve electronic data because its effectiveness is generally based on the comparison of databases containing large volumes of transactional data.

Related to data matching is *data linkage*, also known as *data profiling*, which is a computerized use of personal information from a variety of sources, including

personal information banks, to merge and compare files on identifiable individuals or categories of individuals for administrative purposes. This linkage or profiling activity generates a new body of personal information.

Data matching and data linkage may have a valuable role to play in increasing the efficiency of a wide variety of public body programs. They can, however, also have a major impact on the privacy of individuals. For this reason, there is a need to balance the requirements for efficiency in public body programs with the potentially invasive nature of the activity, particularly data linkage. Careful attention needs to be given to the quality and reliability of the data being matched or linked, especially if the purpose of the activity is to pursue administrative actions against individuals.

Public bodies that are custodians under the *Health Information Act* must comply with relevant sections of that Act when they are considering any data matching activities. A custodian cannot collect health information to be used in data matching, or use or disclose health information to be used in data matching or created through data matching in contravention of the *Health Information Act*. For example, there are specific requirements in that Act for privacy impact assessments when a custodian is performing data matching by combining information in its custody or under its control with information in the custody or under the control of another custodian or a non-custodian.

Public bodies that are custodians under the *Health Information Act* may refer to sections 5.4 and 5.2.7 of Chapter 5 of the *Health Information Act Guidelines and Practices Manual*, published by Alberta Health and Wellness, for more information on the rules for data matching as they apply to health information in the custody or under the control of custodians.

When carrying out data matching, public bodies should

- determine whether the collection, use and disclosure of the personal information that is the subject of the data matching is permitted by provisions of **Part 2** of the *FOIP Act*;
- prior to initiating a matching program, conduct a preliminary assessment of the feasibility of the proposed matching, including the potential impact on the privacy of individuals and the costs and benefits of the data matching program;
- notify the Information and Privacy Commissioner of a new matching program by providing that Office with a copy of this assessment at least 60 days before the program is to commence;
- ensure that data matching programs are authorized by the head of the public body or the designated official to whom this authority has been delegated;
- ensure that all matching activities are accounted for in relevant personal information bank descriptions; and
- verify information generated by a matching program against original or additional authoritative sources before that information is used for an administrative purpose.

Public bodies that are not custodians do not need to conduct a preliminary assessment or send the assessment to the Commissioner if the matching involves

- information not used for an administrative purpose directly affecting an individual;
- two or more databases of information collected and held by the same public body for the same purpose;
- programs that review the contents of a records system to remove or correct items where there is no intention to take administrative action;
- programs that co-locate items previously in separate locations, provided the purposes for which the information collected or compiled continue to apply; or
- information used for research, statistical or program evaluation purposes, if the output is in a form that is not individually identifying, provided **section 42** has been complied with.

### ***Preliminary assessment***

When considering a data matching program, a preliminary assessment should be carried out to determine whether matching data is the most practical and convenient approach to the need and whether there is a basis for proceeding in **Part 2** of the *FOIP Act*. The following are the steps for preliminary assessment of a matching program.

- Assess the advantages of the proposed matching program against alternative control, management or enforcement approaches.
- Verify that the collection involved in a matching program is authorized by a statute or regulation of Alberta or Canada, is for the purpose of law enforcement, or relates directly to and is necessary for an operating program or activity of a public body (**section 33**).
- Examine the possibility of collecting the information directly from the individual to whom it relates or whether collection through data matching is permissible under the *FOIP Act*. Indirect collection is permitted if the individual has authorized indirect collection, the public body could obtain the information from another source without the consent of the individual under **section 34(1)**, or direct collection might result in the collection of inaccurate information (**section 34(3)**).
- Determine whether it is necessary to notify individuals of the new use of their personal information, and if so, the best procedures for notification, or if not, the justification for not notifying the individual (**section 34(2)**).
- Describe the means for ensuring that the information used in the matching program, as well as the information generated, is accurate and complete (**section 35**).
- Determine whether the consent of individuals to the use or disclosure of their personal information is required, and if so, the procedures for obtaining any required consent, or if not, the reason for not obtaining consent (**section 40(1)(d)**).
- Determine whether there is other authority for the use or disclosure of the personal information under **section 39** or **40**.
- Set the start and completion dates for the matching program and, where applicable, the schedule for any required periodic or continuing matching programs.

- Describe the results of any pilot projects designed to test the proposed matching programs (whenever possible, matching public bodies should test the programs to evaluate their effectiveness).
- Determine the costs and the benefits of the proposed data-matching program.

At this stage, the public body should also determine the procedures available to

- establish a records retention and disposition schedule for information used in matching programs, including the program protocols used to establish the link between sets of personal information;
- ensure that any new use or disclosure of personal information is included in the directory of personal information banks held by the public body; and
- establish a personal information bank for the personal information generated as a result of the matching program.

#### ***Cost–benefit analysis***

A second step is a basic cost–benefit analysis. Public bodies should determine the costs of a matching program relative to its benefits. This analysis should be in terms of the level of a public body’s resources (e.g. staff, equipment and materials needed to perform a matching program) and the amount of effort required to develop and to implement it. The importance of the cost–benefit factor to the decision to proceed with a matching program will vary with the context in which the public body operates. Projected or actual resource expenditures should be examined in relation to direct costs, data processing and telecommunications costs, administrative overhead, and any costs associated with contracting out activities.

The cost–benefit analysis should quantify and document the following savings, as appropriate:

- funds that may be recouped through voluntary repayments or formal collection action;
- savings due to termination of ineligible benefits;
- savings due to the denial of benefits that would otherwise have been approved;
- savings due to the deterrent effect of the program; and
- savings relative to other methods of data collection or compilation.

It may be appropriate in some instances to provide evidence of a substantive impact on society or the economy that would result if the program were not implemented.

#### ***Notification of the Information and Privacy Commissioner***

As a third step, public bodies should consult with the Office of the Information and Privacy Commissioner on data matching projects. To allow for this external review before implementation, public bodies should give the Information and Privacy Commissioner advance notification of their intention to initiate a matching program. Providing the Commissioner’s Office with the preliminary feasibility assessment may serve this purpose.

A reasonable time frame for such notification is at least 60 days before the matching is scheduled to begin. This ensures that the Office of the Information and Privacy Commissioner is informed of new consistent uses and new data matches. After the review, the Commissioner may advise the head of the public body that, in his or her opinion, the uses or activities are not in accordance with the provisions of the *FOIP Act*.

### **Approval**

A fourth step is to get final approval for the matching activity or program within the public body that is the matching recipient. It is recommended that the final approval for a data matching program be given by the head of the public body undertaking the program or by a senior official specifically delegated under the *FOIP Act* to authorize such programs.

When a public body is frequently involved in matching activities and the size and organization of the body merit it, the head may establish an internal review body. This might consist of senior program officials, information management or information technology staff and the FOIP Coordinator. The group would review proposed matching programs for compliance with **Part 2** of the *FOIP Act* and make recommendations to the head concerning matching programs for which the public body is either the matching recipient or the matching source.

### **Public notification of a matching program**

The *FOIP Act* requires that a public body account publicly for the use and disclosure of personal information. One way to do this effectively is to notify the general public, or specific groups of clients, of a matching program. The inclusion of current, accurate information about all ongoing data matching activities in the directories of personal information banks held by public bodies is an effective way of providing public notification.

### **Special conditions relating to the disclosure of information for matching programs**

When a public body is asked to disclose personal information for data matching purposes (a matching source), there are a number of factors that must be taken into consideration. Disclosure of personal information requested for matching purposes can only be made under the conditions set out in **Part 2** of the *FOIP Act*.

The public body disclosing the information should

- request and review the preliminary assessment and any other available documentation on the proposed matching to assist in making an informed judgment as to whether the proposed match is justified by program needs as well as the requirements of the Act. The public body must be able to demonstrate that it can disclose the information under **section 40** of the Act;
- determine whether additional information or action will be required for verification purposes and whether such disclosure or action is acceptable;
- ensure that when a disclosure is made for matching purposes, it is sanctioned by a written agreement signed by senior officials representing both the matching



source and the matching recipient. The agreement should include any further conditions that should apply; and

- ensure that any contract involving a matching program stipulates that the contracted activities will be conducted in accordance with the provisions of the *FOIP Act* and the public body's policy on data matching.

#### **Verification process**

It is a good administrative practice for public bodies to subject information generated by a matching program to a verification process involving original or additional authoritative sources. This verification process should be carried out before the information is used in decision-making that directly affects an individual.

Furthermore, an individual should be given an opportunity to refute the information produced by a matching program before any administrative action concerning the individual is taken.

#### **Security**

Personal information and computer systems should be safeguarded from accidental and deliberate threats to confidentiality and to data integrity, including authenticity, accuracy, currency, and completeness. Security safeguards implemented by the matching recipient should be at least equivalent to those of the matching source.

#### **Retention and disposition**

A matching recipient should establish retention and disposition standards for personal information used and generated by a matching program. These standards are established through records retention and disposition schedules or agreements.





## 10.

# INFORMATION AND PRIVACY COMMISSIONER

### Overview

This chapter covers

- the appointment, mandate, general powers and monitoring role of the Information and Privacy Commissioner;
- disclosure of information to the Commissioner;
- investigations, reviews and inquiries;
- judicial review of Commissioner's Orders; and
- the adjudication process and powers of an adjudicator under the Act.

### 10.1

#### Appointment

The Information and Privacy Commissioner is an Officer of the Legislature and is independent of government. **Section 45** of the *FOIP Act* provides that the Lieutenant Governor in Council, on the recommendation of the Legislative Assembly, must appoint an Information and Privacy Commissioner to carry out the duties and functions set out in the Act.

The Commissioner is appointed for a term not exceeding five years and is eligible for reappointment. The Commissioner may not be a Member of the Legislative Assembly (**section 45(3)**). The Commissioner may resign, but may be removed or suspended from office only for cause or incapacity (**section 47**). This means that the Commissioner may not be removed by arbitrary or capricious action, but only for some reason affecting or concerning the ability or fitness of the Commissioner to perform the duties of the office.

### 10.2

#### Mandate and General Powers

**Part 4** of the *FOIP Act* establishes the position of Information and Privacy Commissioner, the supporting office, and the general powers of the Commissioner. These provisions fulfil one of the purposes of the Act, namely, that the Act provide for independent reviews of decisions made by public bodies under the Act and the resolution of complaints under the Act (**section 2(e)**).

The Office of the Information and Privacy Commissioner was established in Alberta in 1995. The Commissioner has a continuing responsibility to ensure that public bodies are complying with the letter and spirit of the Act.

The general powers of the Commissioner are listed in **section 53**. The Commissioner has general responsibility for monitoring how the legislation is administered to ensure that its purposes are achieved. Specifically, the Commissioner may

- conduct investigations to ensure compliance with any provision of the Act or compliance with rules relating to the destruction of records; this includes destruction in accordance with rules set out in any other enactment of Alberta, in a bylaw, resolution or any other instrument by which a local public body acts, or as authorized by the governing body of a local public body (**section 53(1)(a)**);

- make an Order regarding duties imposed by the Act, time extensions, fees, or the collection, correction, use, disclosure or destruction of personal information, as described in **section 72(3)**; such an Order can be made whether or not a review is requested (**section 53(1)(b)**);
- inform the public about the Act (**section 53(1)(c)**);
- receive comments from the public concerning the administration of the Act (**section 53(1)(d)**);
- engage in or commission research into anything affecting the achievement of the purposes of the Act (**section 53(1)(e)**);
- comment on the implications for access to information or protection of personal privacy of proposed legislative schemes or programs of public bodies (**section 53(1)(f)**);
- comment on the implications for protection of personal privacy of using or disclosing personal information for record linkage (**section 53(1)(g)**);
- authorize the collection of personal information from sources other than the individual the information is about (**section 53(1)(h)**);
- bring to the attention of the head of a public body any failure to assist applicants under **section 10** (**section 53(1)(i)**); and
- give advice and recommendations of general application to the head of a public body on matters respecting the rights or obligations of a head under the Act (**section 53(1)(j)**).

Further, without limiting the general powers in **section 53(1)**, the Commissioner may investigate and attempt to resolve complaints from the public that

- a duty imposed by **section 10** (duty to assist applicants) has not been performed (**section 53(2)(a)**);
- an extension of time for responding to a request is not in accordance with **section 14** (time extensions) (**section 53(2)(b)**);
- a fee required under the Act is inappropriate (**section 53(2)(c)**);
- a correction of personal information requested under **section 36(1)** has been refused without justification (**section 53(2)(d)**); and
- personal information has been collected, used or disclosed by a public body in contravention of **Part 2** of the Act (**section 53(2)(e)**).

The Commissioner does not have the power to investigate whether information other than personal information has been improperly disclosed outside the request process under **Part 1** of the Act (*IPC Order 2001-035*).

The Commissioner has sole jurisdiction to investigate or review matters of access to information and privacy protection that are governed by the Act. The Act specifically prohibits the Ombudsman from investigating any matter within the jurisdiction of the Commissioner unless the Commissioner agrees (**section 62**).

As an independent Officer of the Legislature, the Commissioner reports annually to the Legislative Assembly, describing the work of the Commissioner's Office, any complaints or reviews resulting from a decision, act or failure to act of the



Commissioner as head of a public body, and other matters relating to freedom of information and protection of personal privacy (**section 63**).

Further information, including copies of brochures, news releases, Orders, Investigation Reports, Practice Notes, and Annual Reports, is available on the website of the Office of the Information and Privacy Commissioner ([www.oipc.ab.ca](http://www.oipc.ab.ca)).

### 10.3 Monitoring Role

The Information and Privacy Commissioner may investigate the administration of the Act by public bodies. The Commissioner may also audit the practices of public bodies in the areas of access to information and protection of privacy.

In the area of access to information, the Commissioner may, for example,

- examine a public body's compliance with the time limits imposed by the Act;
- investigate allegations that records are being destroyed to avoid producing them in response to a request under the Act; or
- investigate whether a public body is acting appropriately in the disclosure of information in the public interest under **section 32**.

In the area of privacy protection, the Commissioner may, for example,

- investigate a public body's disclosures of personal information to third parties to ensure that the disclosures are in accordance with the requirements of **section 40** of the Act;
- review the collection of personal information by a public body to ensure that the public body has the legal authority to collect the information (**section 33**) or is complying with the rules for indirect collection (**section 34**);
- review the records disposition practices of a public body to ensure that it is retaining personal information as required by **section 35(b)** of the Act;
- audit a public body's procedures within a program or personal information system to ensure compliance with **Part 2** of the Act;
- investigate the application of new information technology to ensure that privacy rights of individuals are being adequately addressed and protected; or
- review and comment upon a privacy impact assessment conducted by a public body when the public body is developing or enhancing a program, administrative practice or information system that may have an impact on an individual's privacy.

The Commissioner may also examine and comment on legislation and program activities in terms of any implications for access to information and protection of privacy. Examples of such legislation and program activities include:

- the amendment of a statute or regulation to include provisions for introducing personal identifiers, or to allow release of personal information. The Commissioner could examine the public body's reasons for including such amendments and comment on their relationship to the provisions and intent of the *FOIP Act*; and

- changes to programs that involve an expansion of the amount of personal information that is collected (e.g. for security screening), data matching (e.g. to verify eligibility for a program), the use of new information technology for program administration (e.g. smart cards), changes in service delivery (e.g. call centres), and the application of the Act to public body contracts with the private sector, including organizations outside Alberta.

By commenting on and informing the public about the implications of legislative and other proposals of public bodies, the Commissioner can help public bodies to comply with the spirit of open government and privacy rights and to be accountable for their actions.

The Commissioner also has the mandate to conduct or commission research into any issue affecting the way in which the Act's purposes are being achieved.

The Commissioner's role in dealing with reviews and complaints from persons not satisfied with the handling of a FOIP request or correction of personal information is discussed in section 10.7 of this chapter.

---

#### 10.4 Provision of Advice

The Information and Privacy Commissioner may provide the head of a public body with advice and recommendations on matters respecting the rights or obligations of a head under the Act (**section 53(1)(j)**). Further, the head of a public body may ask the Commissioner to give advice and recommendations on any matter respecting any rights or duties under the Act (**section 54(1)**).

The Commissioner may include advice or recommendations in an Order or an Investigation Report. The head of a public body might seek advice from the Commissioner on general procedures, or matters of interpretation relating to an access request or the proper application of the privacy protection provisions of **Part 2** of the *FOIP Act*. The advice will normally be sought through a letter from the head of a public body to the Commissioner. Advice given in response to a request from the head of a public body will normally be of a general nature and not anticipate or relate to a specific case. Advice can include recommendations on the administration and application of the Act generally in a particular public body.

**Section 54(2)** provides that the Commissioner may respond to the head of a public body, in writing, with advice and recommendations that

- state the material facts either expressly or by incorporating facts stated by the head;
- are based on these facts; and
- are based on any other considerations that, in the opinion of the Commissioner, are appropriate.

---

#### 10.5 Disclosure to the Commissioner

As discussed in section 2.9 of Chapter 2, **section 82(2)** of the Act requires the Information and Privacy Commissioner to investigate and review any disclosure made to the Commissioner by a public body employee of any information that an employee is required to keep confidential and that the employee, acting in good faith, believes

- ought to be disclosed by a head under **section 32** (disclosure in the public interest); or
- is being collected, used or disclosed in contravention of **Part 2** of the Act.

The Commissioner must not disclose the identity of the employee to any person without the employee's consent (**section 82(3)**). In carrying out an investigation and review under this provision, the Commissioner has the powers of investigation, mediation and order-making, as well as the protections provided under **Part 4** of the Act (**section 82(7)**).

For example, in *IPC Investigation Report F2003-IR-004*, allegations made to the Commissioner by Government of Alberta employees about improper collection and use of their personal information in an employee satisfaction survey were investigated under **section 82(2)**.

If an employee of a public body, acting in good faith, discloses information to the Commissioner or exercises any other right under **section 82**, the public body must not take any adverse employment action against the employee (**section 82(5)**). A public body employer that contravenes **section 82(5)** is guilty of an offence and liable to a fine of not more than \$10,000 (**section 82(6)**).

## 10.6

### Powers, Privileges and Immunities

#### Powers under the *Public Inquiries Act*

The Information and Privacy Commissioner has all the powers, privileges and immunities of a commissioner under the *Public Inquiries Act* and the powers under **section 56(2)** of the *FOIP Act* when conducting an investigation under **section 53(1)(a)**, an inquiry under **sections 69** or **74.5**, or in giving advice and recommendations under **section 54** of the *FOIP Act*. These include the power to compel witnesses to attend and answer questions at an inquiry, to compel records to be produced, to hold a person in contempt, and to obtain assistance from law enforcement officers.

#### Power to compel production of records

The Commissioner may require any record to be produced and may examine any information in a record, including personal information, whether or not the record is subject to the provisions of the Act (**section 56(2)**) (see *IPC F2006-021*).

A public body must produce any record or copy of a record requested by the Commissioner under **section 56(1)** or **(2)** within 10 days. Records must be produced despite any privilege of the law of evidence that might otherwise apply (**section 56(3)**). The Commissioner has established a protocol as to how his Office will deal with records for which a public body has claimed solicitor–client privilege (see *Solicitor–Client Adjudication Protocol*, published on the Commissioner's website).

The requirement to produce records applies to records that the public body believes to be excluded from the coverage of the Act under **section 4(1)** (see *IPC FOIP Practice Note 4: Section 4 – Exclusions from the Act*).

A public body also must produce records despite any other enactment of Alberta that prohibits disclosure, but not if a federal Act, such as the *Youth Criminal Justice Act*, prohibits disclosure (see *IPC Order 96-015*).

If a public body is required to produce a record and it is not practicable to make a copy of it, the head of a public body may request that the Commissioner examine the original at the site of the public body (**section 56(4)**).

The Commissioner must return all records or copies of records to the public body after completing a review or investigating a complaint (**section 56(5)**).

### **Power to disregard requests**

The head of a public body may, under **section 55** of the *FOIP Act*, request the Commissioner's authorization to disregard requests from an applicant. This applies to both requests for access to information and requests for correction of personal information. The public body must present facts in support of its request. The Commissioner then makes a decision. Refer to section 3.2 of Chapter 3 for more information on how a public body makes such a request and what supporting information must be provided to the Commissioner.

### **Statements provided to the Commissioner**

A statement made or an answer given by a person during an investigation or inquiry by the Commissioner is inadmissible in evidence in court or in any other proceeding, except

- in a prosecution for perjury in respect of sworn testimony;
- in a prosecution for an offence under the *FOIP Act*; or
- in an application for judicial review or an appeal from a decision of that review (**section 57(1)**).

These conditions also apply to evidence from proceedings conducted before the Commissioner (**section 57(2)**). Anything said, any information supplied or any record produced by a person during an investigation or inquiry by the Commissioner is privileged; the rules that apply are those for a proceeding before a court (**section 58**).

The phrase *a statement made during an inquiry* was held by the Commissioner's Office to include a statement made in an agent's request for review letter, which initiated the inquiry process. The inquiry, as an adjudicative process, was held to be a *proceeding* for the purposes of **section 57(1)** (see *IPC Order 2001-032*).

**Section 59** of the Act places restrictions on the disclosure of information by the Commissioner and the staff of the Office of the Information and Privacy Commissioner. They must not disclose any information they obtain in the performance of their duties, with the following exceptions:

- the Commissioner may authorize disclosure of information that is necessary for the conduct of an investigation under the Act or to establish the grounds for findings and recommendations made under the Act (**section 59(2)**);

- the Commissioner may disclose to the Minister of Justice and Attorney General information relating to the commission of an offence against an enactment of Alberta or Canada, if the Commissioner believes there is sufficient evidence to justify such disclosure (**section 59(4)**) (see *IPC Order 2001-033*); and
- the Commissioner may authorize disclosure of information in the course of a prosecution for perjury or for an offence under the Act, or in an application for judicial review or an appeal arising from that application (**section 59(5)**).

This section allows the Commissioner to request that the police lay charges under **section 92** of the Act.

During the conduct of an investigation, inquiry or audit, the Commissioner and the staff of the Commissioner's Office must not disclose any information that the head of a public body would be required or authorized to withhold from disclosure. They must also ensure that they do not disclose the fact that information exists where, in the notice of refusal to provide access, the public body did not indicate whether or not the information existed (**section 59(3)**) (see *IPC Order F2006-012*).

### Protection from liability

The Commissioner and the staff of the Commissioner's Office are not liable for anything they do, report or say in good faith in the exercise of their duties under **Part 4** of the Act (Office and Powers of the Information and Privacy Commissioner), or **Part 5** of the Act (Review and Complaints) (**section 60**).

As long as the Commissioner and the Commissioner's staff act honestly and with the intention of complying with the Act, no action can be brought against them.

### Delegation of the Commissioner's powers

**Section 61(1)** provides that the Commissioner may delegate, in writing, to another person any duty, power or function of the Commissioner under the Act. The only exception to this provision is that the Commissioner cannot delegate the power to delegate.

This allows the Commissioner to delegate, for example, the power

- to examine law enforcement information and Cabinet documents,
- to authorize public bodies to disregard requests, and
- to hold inquiries and issue Orders on completion of those inquiries.

## 10.7 Reviews

**Section 65** of the *FOIP Act* provides persons who have made a FOIP request with the right to ask the Information and Privacy Commissioner to review any decision, act or failure to act of the head of a public body that relates to the request (**section 65(1)**).

Third parties have the right to ask the Commissioner to review the decision of a public body to provide access to records where disclosure might be an unreasonable invasion of their personal privacy under **section 17** or might harm their business interests under **section 16**. If the public body decides to grant access in response to a request under **Part 1** of the Act, a third party that has been given notice under the Act



may request a review before any records or parts of records are disclosed (**section 65(2)**). A third party does not have the right to review by the Commissioner of the sufficiency of a third party notice (*IPC Order 99-023*).

A person who believes that his or her personal information has been collected, used or disclosed in contravention of **Part 2** of the Act may also ask the Commissioner to review the matter (**section 65(3)**). Only an individual whose personal information has allegedly been collected, used or disclosed in contravention of **Part 2** has a right to request a review under **section 65(3)** (*IPC Order 2001-004*). The individual initiating the complaint has the onus of establishing that he or she has standing to bring the complaint and of providing evidence that suggests that his or her personal information has been collected, used or disclosed (*IPC Order F2007-019*).

The surviving spouse or adult interdependent partner or a relative of a deceased individual may ask the Commissioner to review a decision of the head of a public body under **section 40(1)(cc)** not to disclose personal information about the deceased individual (**section 65(4)**).

The right to an impartial review of decisions or actions of a public body is fundamental to guaranteeing access to information and protection of privacy rights. The review mechanism ensures that these rights are interpreted consistently among public bodies and the purposes of the Act are achieved. Commissioner's Orders, which summarize the issues, arguments, findings and reasons of the Commissioner, also provide guidance to public bodies regarding the proper interpretation of the Act.

A review by the Commissioner of the decision of a public body is intended to be an avenue of last resort. In most cases, a person will be satisfied that the public body has acted responsibly and any outstanding issues can be settled between the public body and the person concerned. Even in cases where the person asks the Commissioner to review a decision, issues can often be settled through mediation and an inquiry may not be necessary.

Certain matters that may be the subject of a request for review can also be grounds for a complaint to the Commissioner under **section 53(2)** of the Act. These are

- matters relating to the public body's duty to assist the applicant (**section 10**);
- a decision to extend the time limit under **section 14** for responding to a request;
- the amount of a fee charged or the refusal to waive all or part of a fee under **section 93**;
- a refusal to make a correction to personal information, as requested under **section 36(1)**; and
- the collection, use or disclosure of personal information in contravention of **Part 2** of the Act.

### Requesting a review

**Section 66** of the Act sets out the process for requesting a review. A flowchart of the review process is provided in Figure 13. The Office of the Information and Privacy Commissioner provides a **Request for Review Form** for this purpose. A copy of the form is included in Appendix 5 of this publication.

Applications for a review can be made on this form or by letter, but in all cases must be in writing. **Section 84** establishes classes of individuals who may act for deceased persons, incompetent persons, minors and any other individuals in exercising this right under the Act. (See section 2.5 of Chapter 2 for a discussion of the exercise of rights by others.)

A person must deliver a request for a review to the Commissioner within 60 days of receiving notification of a public body's decision or a longer time when allowed by the Commissioner (**section 66(2)(a)**). Third parties have 20 days in which to seek a review (**section 66(2)(b)**). The Commissioner has no ability to allow a third party a longer period of time to request a review.

Failure by a public body to respond in time to a request for access to a record is treated as a decision to refuse access (deemed refusal). In this case, because there has not been any notification by the public body, the 60-day time limit does not apply.

### **Preparation for a review**

A public body must be able to show that it has properly fulfilled its duties under the Act. It should document the reasons for each decision relating to the withholding of records, or parts of records, and should ensure that the circumstances surrounding the request and the provisions of the Act support each action it takes.

To reduce the need for review of decisions, public bodies should provide applicants and third parties with clear explanations of their decisions, the provision(s) of the Act that apply and the reasons why they are applicable in the particular instance. These explanations provide a basis for discussion of the decision and may help the public body and the person to settle any outstanding issues without recourse to the Office of the Information and Privacy Commissioner. This point is discussed in IPC FOIP Practice Note 2: *Informing the Applicant of Grounds for Refusal*.

If a particular case for review deals with an issue that has implications across government or affects most public bodies, the public body should consult with Access and Privacy, Service Alberta.

### **Review process**

The *FOIP Act* has a number of provisions governing the review process. In addition, the Office of the Information and Privacy Commissioner has developed procedures for conducting reviews and inquiries and these are available from that Office. See, in particular, IPC FOIP Practice Note 5: *Preparing Records and Submissions for Inquiries*.

Upon receiving a request for review, the Commissioner must provide a copy of the request to the head of a public body and to any other person who, in the opinion of the Commissioner, is affected by the request. The Commissioner must also provide to these persons, and to the person who requested the review, a summary of the review procedures and an anticipated date for a decision (**section 67(1)**).

The Commissioner may sever any information in the request that is considered appropriate before providing copies as stated above (**section 67(2)**). This is necessary

because applicants may include personal information as part of their requests for review, and it may not be appropriate to disclose this to the public body or other persons.

The staff of the Commissioner's Office, the public body and the applicant or third party will jointly review the request for review to determine whether or not the concerns raised in it can be addressed through mediation.

The Commissioner will also likely ask the public body to submit copies of the following documentation, where applicable:

- the FOIP request;
- notice of the public body's decision;
- any correspondence related to the request, issue or decision;
- an index of the relevant records and exceptions under the Act relied upon;
- severed and unsevered copies of the records; and, where applicable,
- descriptions of personal information in the public body's personal information banks and policies and procedures for the management of personal information under **Part 2** of the Act.

The public body will initially be more familiar with the issues involved than the Office of the Commissioner. If the public body has any information concerning affected persons who should be notified of the review, it should inform the Commissioner's Office as soon as possible.

The public body should also make known any relevant issues, considerations or factors that affected the making of the particular decision. The Commissioner will have a better understanding of the public body's position if the public body can demonstrate that it made every effort to meet a person's needs and to resolve outstanding issues.

### **Mediation**

**Section 68** provides that the Commissioner may authorize a mediator to investigate and try to settle any matter that is the subject of a request for a review. In most cases, the Commissioner will instruct a portfolio officer to proceed in this way. The mediator does not impose a settlement. Rather, mediation is intended to help the public body and the person requesting a review arrive at a settlement, which may resolve matters at issue so that a formal inquiry is not required.

If matters are not settled at mediation and these matters proceed to inquiry, the findings of the portfolio officer are not considered or adopted into the inquiry. Instead, the parties are given an opportunity to present fresh evidence and arguments before the Commissioner (*IPC Order F2004-024*).

### **Inquiry**

If a mediator is not appointed, or the matter is not resolved with the help of a mediator, the Commissioner must conduct an inquiry unless **section 70** applies (**section 69(1)**). **Section 70** specifies circumstances under which the Commissioner

may refuse to conduct an inquiry. In the course of the inquiry, the Commissioner will decide all questions of law and fact.

The Commissioner's powers in conducting inquiries are set out in **sections 56 and 69** of the Act. The Commissioner has broad discretion to determine how an inquiry will be conducted. It may be conducted in private (**section 69(2)**), and the Commissioner may decide whether representations are to be made orally, or in writing or a combination of the two (**section 69(4)**).

The person who asked for the review, representatives of the public body concerned, and any person given a copy of the request for review are entitled to make representations to the Commissioner during the inquiry (**section 69(3)**). They may choose to be represented by counsel or an agent (**section 69(5)**).

No party has a right to be present during another party's representations, or to have access to or to comment on representations made by another person during the inquiry process (**section 69(3)**). *Representations* in this context means the whole of a party's case, including both evidence and legal argument (*IPC Order 2001-039*).

The Commissioner can allow certain evidence to be submitted *in camera*. The Commissioner has ruled that holding *in camera* sessions during oral inquiries does not breach the principle of procedural fairness (*IPC Order 98-006*).

In the case of a refusal of access, the Commissioner has the right to view all records that have been withheld from disclosure in whole or in part. This right pertains regardless of the exception that the public body has used or the fact that the public body believes the records are excluded from the scope of the Act.

The Commissioner may require the records to be produced within 10 days (**section 56(3)**). The Commissioner must return such records to the public body upon completion of the review (**section 56(5)**).

The head of a public body may require the Commissioner to examine a record at the site at which it is being held, if it is not practical to make a copy (**section 56(4)**). This could occur, for example, when a record is too fragile to copy or the copying process would damage the record. Public bodies should avoid, as much as possible, requiring on-site examination of records since this is likely to place an additional administrative burden on their own, and the Commissioner's, operations.

The Commissioner may compel witnesses to attend an inquiry and answer questions. The Commissioner has all the powers of a Commissioner provided under the *Public Inquiries Act*. These include the power to hold a person in contempt and to obtain the assistance of law enforcement officers to compel attendance at an inquiry or to compel records to be produced.

### **Refusal to conduct inquiry**

The Act allows the Commissioner to refuse to conduct an inquiry under certain circumstances. If the Commissioner believes that the subject matter of a request has already been dealt with in an Order or an Investigation Report, the Commissioner may refuse to conduct an inquiry (**section 70(a)**).

For example, in a *Decision Regarding Section 70 of the FOIP Act* in August 2003, the Commissioner agreed with a public body that he had already decided in *IPC Order 2001-007* that the public body had made every reasonable effort to search for and provide the requested records. The Commissioner exercised his discretion to refuse to conduct inquiries into the applicants' requests for reviews.

**Section 70(b)** allows the Commissioner to refuse to conduct an inquiry if, in the opinion of the Commissioner, the circumstances warrant. Consideration might be given to refusing to conduct an inquiry if the Commissioner were satisfied that

- the matter could more appropriately be dealt with by means of a procedure under another law,
- an inquiry would not result in any useful remedy (e.g. because a public body has already disclosed all available records in response to a FOIP request), or
- a request for review is frivolous, vexatious or made in bad faith.

A person who believes that the Commissioner has improperly refused to conduct an inquiry may apply to the Court of Queen's Bench for judicial review of the Commissioner's decision.

#### **Time limits for review**

A review by the Commissioner must be completed within 90 days after receipt of the request for review (**section 69(6)**). This time limit encompasses all elements of the review process, including mediation and any formal inquiry.

However, the Commissioner may extend the period for the review. The Commissioner must notify all parties to a review of the extension and provide an anticipated date for the completion of the review (**section 69(6)**). The intent of the Act is to ensure that an independent review of decisions can take place, so, even if the process is not completed within the extended time limit, the Commissioner has the power to complete the inquiry (see *IPC Order 99-011*).

In *Business Watch International Inc. v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 10, the Court of Queen's Bench determined that the Commissioner did not lose jurisdiction to continue a review when there had been non-compliance with the requirements of **section 69(6)**. The Court found that, in the circumstances of the case, it was reasonable for the Commissioner to conclude that the 90-day statutory time period was directory, not mandatory. Relevant circumstances included the fact that the decision involved the potential loss of jurisdiction rather than the taking of jurisdiction, the complainant did not complain about the delay, and that if the process was terminated, it could be easily re-instituted. (See also *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 268.)

#### **Burden of proof**

**Section 71** establishes where the burden of proof lies in various situations relating to access to records. Generally, the burden of proof rests with the public body refusing



access to all or part of a record (**section 71(1)**), unless the request is for a record or part of a record that contains personal information about a third party.

This means that, under most circumstances, the public body must prove, on a balance of probabilities, that particular information may or must be excepted from disclosure under the Act or that information in records responsive to a request is excluded from the scope of the Act.

Careful documentation of the reasons for refusing to disclose information in responsive records will provide the basis for meeting the burden of proof.

When a public body has refused to disclose personal information under **section 17**, which requires public bodies not to disclose personal information if the disclosure would be an unreasonable invasion of an individual's privacy, the burden of proof rests with the party requesting disclosure of the personal information. The applicant requesting the personal information must show that disclosure would not be an unreasonable invasion of the personal privacy of the individual to whom the information relates (**section 71(2)**).

When a third party has requested a review of a public body's decision to disclose a record or part of a record containing personal information about the third party, the burden of proof also lies with the applicant who has requested disclosure of the personal information. The applicant must show that disclosure would not constitute an unreasonable invasion of the third party's personal privacy (**section 71(3)(a)**).

When the inquiry concerns a public body's decision to disclose third party business information (**section 16**), the burden of proof lies with the third party resisting disclosure. That is, the third party must demonstrate that the applicant has no right of access to the record (**section 71(3)(b)**).

For more information on this topic, including a table setting out the way the Commissioner has ruled on who has the burden of proof under different sections of the Act, refer to FOIP Bulletin No. 9: *Burden of Proof*, published by Access and Privacy, Service Alberta.

### **Commissioner's Orders**

Upon completion of an inquiry, **section 72** of the Act requires the Commissioner to make an Order. If the inquiry concerns a refusal to grant access to all or part of a record, the Commissioner must order one of the following:

- require the public body to give access to all or part of the record;
- confirm the decision of the public body or require the head to reconsider a decision to refuse disclosure; or
- require the head to refuse access to part or all of the record requested.

When the Commissioner finds that a refusal to grant access is authorized under the Act, and the head of the public body has properly exercised his or her discretion, the Commissioner can only confirm the decision of the public body or request that the head reconsider the decision.

The Commissioner can require the head of a public body to reconsider only a decision to *refuse* access, not a decision to *grant* access (*IPC Orders 98-001 and F2005-016*).

If the inquiry concerns any other matter, the Commissioner may make an Order requiring compliance with the applicable provision(s) of the Act, as listed in **section 72(3)**.

The Commissioner only has the authority to make an Order against a public body, not against another party (*IPC Order F2003-004*).

**Section 72(4)** provides that the Commissioner may specify any terms or conditions in an Order. A copy of the Order is given to the person who asked for the review, the head of the public body concerned, any person given notice of the review under **section 67** of the Act, and the Minister responsible for the administration of the Act.

The head of a public body that has received an Order from the Commissioner must comply with that Order no earlier than 45 days and no later than 50 days after receiving it (**sections 74(1) and (2)**). This is to allow an applicant, a third party or the public body time to apply for judicial review. If an application for judicial review is made, the Commissioner's Order is stayed until the Court has dealt with the application (**section 74(4)**).

In practice, the Commissioner will normally courier copies of the Order to all parties at the same time and will not review a file for a letter of compliance until after day 50. The Court has the power to extend the 45-day time limit for applying for judicial review if it considers an extension appropriate.

There is no appeal from an Order made by the Commissioner (**section 73**), except a limited appeal through judicial review (see section 10.10 of this chapter).

It is an offence to fail to comply with an Order made by the Commissioner under **section 72**. The Commissioner may choose to file a copy of an Order with the clerk of the Court of Queen's Bench and, after filing, the Order is enforceable as a judgment or Order of that Court (**section 72(6)**).

Copies of the Commissioner's Orders are available on the Commissioner's website.

---

## 10.8 Investigations

**Section 53(1)** of the *FOIP Act* enables the Information and Privacy Commissioner to monitor compliance with the Act and carry out investigations into how the Act is being administered to ensure that its purposes are achieved. **Section 53(2)**, without limiting these more general powers, enables the Commissioner to investigate and attempt to resolve complaints that

- a duty imposed by **section 10** (duty to assist) has not been performed;
- an extension of time for responding to a request is not in accordance with **section 14**;
- a fee under the Act is not appropriate;
- a correction of personal information requested under **section 36(1)** has been refused without justification; and

- personal information has been collected, used or disclosed by a public body in contravention of **Part 2** of the Act.

The main difference between an investigation and a review is that an investigation may not be a result of a FOIP request. A complaint that does not arise from a FOIP request is most likely to occur in cases involving disclosure in the public interest or allegations of improper collection, use or disclosure of personal information.

The Commissioner has the general power under **section 53(1)** to initiate an investigation. He does not have to wait until a complaint has been submitted in order to conduct an investigation, especially where there is a possible breach of a provision in **Part 2** of the Act. See, for example, *IPC Investigation Reports 2000-IR-009* (surveys by third parties of students in schools), *F2003-IR-001* (disclosure of children's personal information on adoption website) and *F2005-IR-001* (improper use of police database).

In order to find a breach of **Part 2** of the Act, there must be a satisfactory level of evidence presented in support of the allegation. Otherwise, a public body would be put in the position of having to "prove a negative" (see *IPC Orders F2002-020* and *F2006-016*).

When an investigation is held into an alleged breach of privacy (**section 53(2)(e)**), a portfolio officer in the Commissioner's Office is assigned to investigate the matter. When the investigation is complete, the portfolio officer will issue his or her findings and any recommendations to both parties. The portfolio officer may communicate the findings and recommendations to the parties orally, by a letter of findings or by an Investigation Report. The complainant is asked whether the findings and recommendations satisfy his or her concerns, and the public body is asked to inform the portfolio officer how it will comply with the recommendations.

If the complainant is satisfied with the findings and recommendations, and the public body accepts the recommendations, the portfolio officer will close the file. If an Investigation Report was prepared, the portfolio officer forwards the report to the Commissioner and advises that the complaint has been resolved. The Commissioner's Office then publicly releases the Investigation Report.

If the complainant is not satisfied with the findings and recommendations, he or she can request that the matter proceed to inquiry in accordance with **section 65(3)**. The findings and recommendations of the portfolio officer are not forwarded to the Commissioner. If an Investigation Report was prepared, the report is not forwarded to the Commissioner and is not publicly released. Evidence collected during the investigation is not forwarded to the Commissioner for the inquiry (*IPC Order F2004-024*).

For further details on the process of dealing with complaints, see IPC FOIP Practice Note 7: *Privacy Complaints – Investigations and Inquiries*.

Public bodies are always informed by the Office of the Information and Privacy Commissioner as to whether an issue is subject to a review (**section 65**) or an investigation (**section 53**). The preparation and response to an investigation will be very similar to those outlined for the review process described above (see IPC FOIP

Practice Note 3: *Complaints about Public Bodies – “Reviews” versus “Investigations”*: Sections 51(2) and 62(1)).

Copies of Investigation Reports by the Office of the Information and Privacy Commissioner are available on the Commissioner’s website.

### **Time limits on complaints**

When an investigation arises from a FOIP request, the applicant must deliver the complaint to the Commissioner within 60 days of receiving notification of the public body’s decision (**section 66(2)(a)**). A longer time may be allowed by the Commissioner (**section 66(2)(b)**). When allowing a delay, the Commissioner will consider all relevant circumstances.

The Act does not specify a time limit for privacy complaints, since these do not, for the most part, arise from a FOIP request.

---

#### **10.9 Privacy Compliance Investigations and Audits**

The Information and Privacy Commissioner can take an active role in investigating compliance with **Part 2** of the Act. An investigation can be undertaken as a result of a complaint that personal information is not being collected, used, disclosed or protected in accordance with the provisions of the FOIP legislation.

As well, the Commissioner may decide to conduct an audit of privacy protection in a program of a public body that has custody or control of sensitive personal information. The Commissioner’s practice is to make all Investigation Reports and Privacy Audit Reports public.

Section 9.1 of Chapter 9 suggests a method of reviewing a public body’s protection of personal information to help in determining whether the public body is in compliance with the requirements of **Part 2** of the Act. It also serves as a guide for remedial measures that may be necessary to adequately protect the personal information in its custody or under its control.

---

#### **10.10 Judicial Review**

The Information and Privacy Commissioner has exclusive jurisdiction to conduct a review and investigate complaints against a public body under the *FOIP Act*. Courts do not have the power to issue Orders under the Act.

However, a person may apply to the Court of Queen’s Bench of Alberta to exercise its inherent jurisdiction to review any action or failure to act on the part of the Commissioner. The Court may also review the decisions of the Commissioner for an error of law on the face of the record, jurisdictional error or breach of natural justice (fairness). In addition, a person who believes that the Commissioner has improperly refused to conduct an inquiry (under **section 70**) may apply for judicial review of the Commissioner’s decision.

Application for judicial review of a decision of the Commissioner must be made not later than 45 days after the party applying for judicial review is given a copy of the decision.

The Court has the power to compel the Commissioner to do something or to refrain from doing something and the power to send a matter back to the Commissioner for reconsideration.

A judicial review is not an appeal of the Commissioner's decision. The Commissioner is the final arbiter of questions of fact but is always subject to the overriding jurisdiction of the Court to ensure that the Commissioner acts within his or her authority. A judicial review will result in the Court either affirming or quashing the Commissioner's Order. Where an Order has been quashed, the Court may refer the matter back to the Commissioner for reconsideration.

The issue of judicial deference to the Commissioner has been considered in several decisions, including:

- *Alberta (Minister of Justice) v. Roy* (10 December 1996), Edmonton 9603-16335 (Alta. Q.B.)
- *University of Alberta v. Pylypiuk*, 2002 ABQB 22
- *Shields v. Information and Privacy Commissioner*, 2004 ABQB 353
- *Qualicare Health Service Corporation v. Alberta (Office of the Information and Privacy Commissioner)*, 2006 ABQB 515
- *Stubicar v. Alberta (Office of the Information and Privacy Commissioner)*, 2007 ABQB 480; 2008 ABCA 357
- *Business Watch International Inc. v. Alberta (Information and Privacy Commissioner)* 2009 ABQB 10

#### 10.11 Adjudicator Process

**Section 75** provides for the designation of a judge of the Court of Queen's Bench as an adjudicator. The Lieutenant Governor in Council may designate an adjudicator in situations

- when the matter under review relates to the Commissioner acting as head of a public body (i.e. the head of the Office of the Information and Privacy Commissioner or any other legislative Office of which the Commissioner is the appointed Officer); or
- when, in the Commissioner's opinion, the Commissioner has a conflict of interest in a review or investigation.

For example, the Commissioner may have a conflict if the Commissioner has been a member or employee of the public body that is the subject of the review. The determination that the Commissioner has a conflict of interest is made by the Commissioner. The Commissioner is in the best position to decide whether his or her decision on a particular matter might later be the subject of a judicial review by the Court on the grounds that the Commissioner had a conflict of interest (a reasonable apprehension of bias).

An applicant or third party seeking a review under these circumstances may request, under **section 79(1)** of the Act, that an adjudicator be appointed to conduct the review.



The request for designation of an adjudicator must be in writing and made to the Minister responsible for the *FOIP Act*. The request must be made within 60 days of the person receiving notice of the decision to be reviewed, or 20 days if a third party is challenging disclosure of information. The adjudicator may decide that a longer period should be allowed.

Upon receipt of the request, Access and Privacy, Service Alberta, will prepare the documentation for the Minister to commence the appointment process. Alberta Justice and Attorney General is responsible for requesting the Chief Justice of Alberta to nominate a judge of the Court of Queen's Bench to act as adjudicator.

The Minister responsible for the *FOIP Act* will request that Cabinet authorize the Lieutenant Governor in Council to designate the judge to act as an adjudicator. The Minister must provide a copy of the applicant's request for review, together with a summary of the review procedures that will govern the process, to the adjudicator, the Information and Privacy Commissioner and any other person affected by the request.

An adjudicator has the powers and duties as the Commissioner, as set out in **section 76** of the Act. An adjudicator cannot review an Order of the Commissioner (**section 75(2)**). A copy of the adjudicator's Order must be given to the Commissioner. An Order made by an adjudicator is final (**section 81(6)**). Adjudication Orders are made available on the Commissioner's website.

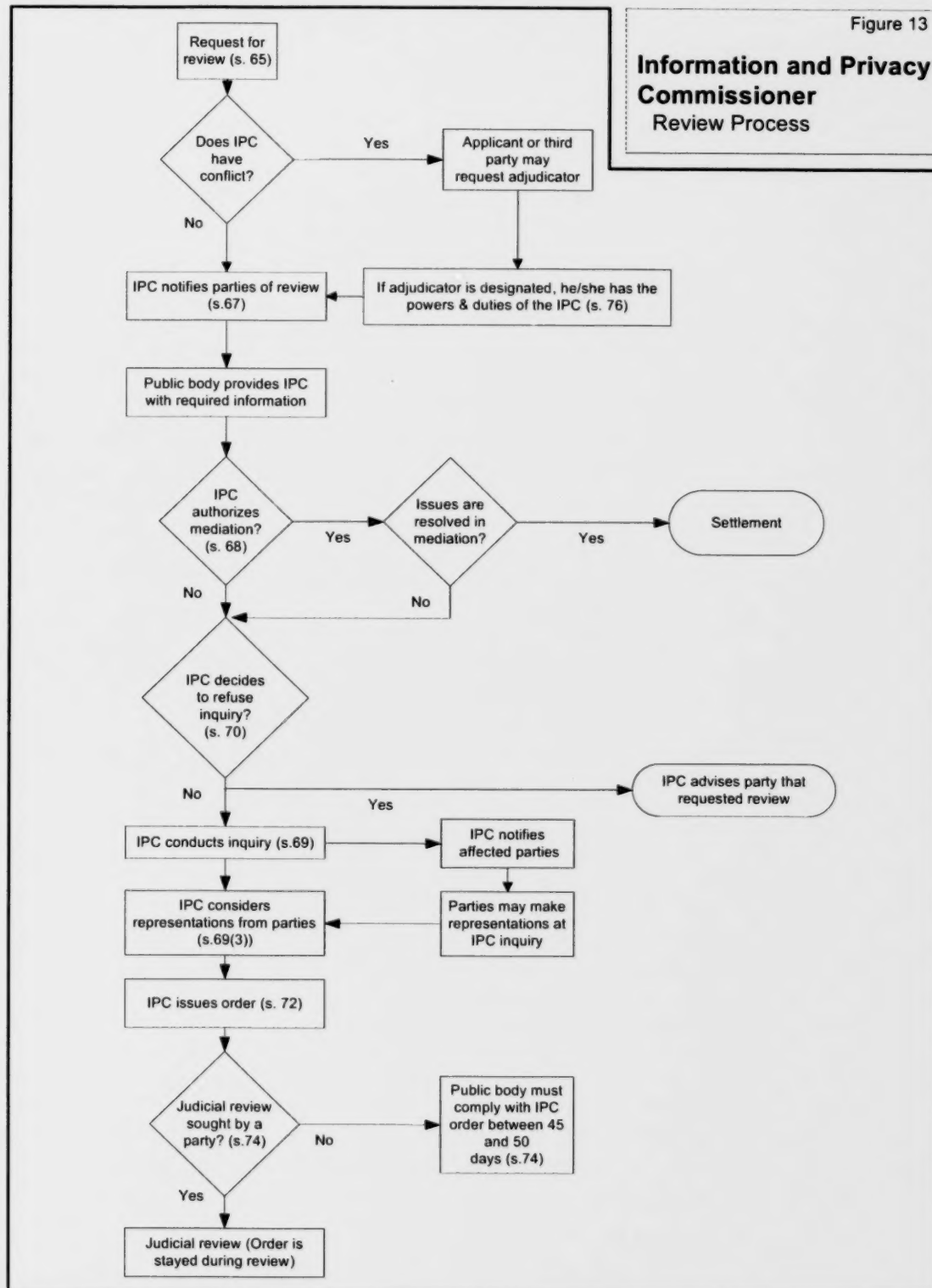
The Minister responsible for the *FOIP Act* is responsible for paying the adjudicator's expenses related to the adjudicator's inquiry.

An application for judicial review may be made in respect of a decision of an adjudicator on the same grounds that a decision of the Commissioner may be reviewed (see section 10.10 of this chapter).

An adjudicator in the Commissioner's Office should not be confused with an adjudicator that has been designated by the Lieutenant Governor in Council for the purposes of **section 75**. The Commissioner may, under **section 61**, delegate one or more persons to act as an adjudicator in his Office to conduct inquiries and issue Orders. The purpose of this delegation is to distribute the Commissioner's workload in the area of inquiries, not to deal with a specific issue of conflict of interest on the part of the Commissioner. The name of "adjudicator" that may be chosen for the delegate is simply an assigned title.

Figure 13

# Information and Privacy Commissioner Review Process











## APPENDIX 1

## DEFINITIONS

This appendix contains a glossary of terms commonly used in administering the *Freedom of Information and Protection of Privacy Act*. Terms defined in the legislation are marked with an asterisk (\*). In many cases, the definition of a term is specific to the particular section of the Act. For further information on words and phrases in the Act that have been defined or considered in Orders of the Information and Privacy Commissioner, see the list at [foip.alberta.ca/legislation/definitions/](http://foip.alberta.ca/legislation/definitions/).

<b>access</b>	The availability of records of a public body for a person to view or copy. The Act provides any person with a right of access to records or to their own personal information that is in the custody or under the control of a public body.
<b>active dissemination</b>	A process whereby information or records are periodically released, without any request, under a program or communications plan. <i>See also</i> <b>routine disclosure</b> .
<b>adjudicator*</b>	A judge of the Court of Queen's Bench of Alberta designated by the Lieutenant Governor in Council to investigate a complaint against the Commissioner as the head of a public body, or to review any decision, act or failure to act of the Commissioner as the head of a public body. An adjudicator may also be appointed when the Commissioner cannot act because of a conflict of interest.
<b>administration of personnel</b>	Refers to activities related to staffing, job classification or compensation, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training and development, occupational health and safety, and separation and layoff. <i>See also</i> <b>management of personnel</b> .
<b>adult interdependent partner</b>	A person who <ul style="list-style-type: none"> <li>lived with the deceased in a relationship of interdependence               <ul style="list-style-type: none"> <li>for a continuous period of not less than three years, or</li> <li>of some permanence, if there is a child of the relationship by birth or adoption,</li> </ul> </li> <li>or</li> <li>entered into an adult interdependent partner agreement with the other person under section 7 of the <i>Adult Interdependent Relationships Act</i>.</li> </ul>
<b>advice</b>	Includes proposals, recommendations, analyses and policy options. For the purposes of the Act's exception for advice from officials, advice should be sought or expected, or be part of the responsibility of a person by virtue of that person's position; be directed toward taking an action; and be made to someone who can take or implement the action.
<b>annotate</b>	Add an explanatory, descriptive or critical note to a record. To annotate personal information with a correction that was requested implies that the correction that was requested appears on the original record, close to the information under challenge by the applicant.
<b>applicant*</b>	Any person who makes a request under the Act for access to a record.

<b>arm's-length transaction</b>	See <b>non-arm's length transaction</b> .
<b>audit*</b>	A financial or other formal and systematic examination or review of a program, portion of a program or activity. See also <b>disclosure for audit purposes</b> .
<b>biometric information*</b>	Information derived from an individual's unique measurable characteristics.
<b>burden of proof</b>	The obligation of one of the parties in an inquiry to persuade the Commissioner to decide an issue in its favour.
<b>Cabinet</b>	The common name for the Executive Council. It consists of a committee of Ministers that acts collectively with the Premier to decide matters of government policy.
<b>commercial information</b>	Relates to the buying, selling or exchange of merchandise or services. Commercial information includes third party associations, history, references, and insurance policies, as well as pricing structure, market research, business plans, and customer records. See also <b>financial information</b> .
<b>Commissioner*</b>	The Information and Privacy Commissioner appointed under the Act. The Commissioner is an Officer of the Legislature and is independent of government.
<b>complaint</b>	<p>A formal expression of dissatisfaction submitted by an applicant or other person to the Commissioner. A complaint may be based on one or more of the grounds specified in the Act:</p> <ul style="list-style-type: none"><li>• a public body has not met its duty to assist;</li><li>• a public body's extension of time for responding to a request is not in accordance with the Act;</li><li>• a fee charged by a public body is inappropriate;</li><li>• a correction of personal information has been refused without justification; or</li><li>• personal information has been collected, used or disclosed by a public body in contravention of the privacy provisions of the Act.</li></ul>
<b>confidence</b>	See <b>in confidence</b> .
<b>confidential source</b>	<p>For the purposes of the Act's exception for law enforcement information, "confidential source" means an informant who provided law enforcement information to a public body and who was either promised confidentiality or who had an expectation of confidentiality based on the circumstances in which the information was provided.</p> <p>See also <b>in confidence</b>.</p>
<b>consultation</b>	<p>The process by which a public body asks employees within the body, other public bodies, individuals, or third parties (including other levels of government) to comment on a request for access to information in which they have an interest.</p> <p>Within the context of the Act's provisions for third party notice, "consultation" refers to the process whereby a public body notifies a third party of a request, receives representations from the third party, and subsequently informs the third party of its decision regarding access to the information in question.</p>

For the purposes of the Act's exception for advice from officials, "consultations" refers to the process where persons having the responsibility to make a decision freely discuss the issues before them in order to arrive at a well-reasoned decision. Such consultations occur when the views of one or more officers or employees is sought as to the appropriateness of particular proposals or suggested actions. *See also* **deliberations**.

**continuing request**

An access request that continues to be in effect for up to two years. A delivery schedule is established with the applicant's agreement, and the request is reactivated at intervals set out in the schedule. Each time the request is processed, records newly in the custody or under the control of the public body since the last delivery are provided to the applicant. *See also* **request**.

**control**

For the purposes of determining whether the Act applies to a record that is "under the control" of a public body, "control" means the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

**custody**

For the purposes of determining whether the Act applies to a record that is "in the custody of" a public body, "custody" means physical possession.

**data matching**

In the context of the Act's provisions relating to personal information, "data matching" refers to the comparison (generally by electronic means) of one or more databases or sets of records of personal information held by one public body or organization with one or more other databases or sets of records held by a different public body or organization, where the matching program creates or merges files on identifiable individuals. Data matching tends to involve electronic data because its effectiveness is generally based on the comparison of databases containing large volumes of transactional data.

**delegation**

The formal process whereby the head of a public body authorizes an employee or officer within the public body to perform certain duties or to exercise certain powers or functions of the head under the Act. A delegation under the Act must be in writing.

**deliberations**

For the purposes of the Act's exception for advice from officials, "deliberations" refers to a discussion of the reasons for and against a future action by an employee or officer of a public body prior to a decision being made. *See also* **substance of deliberations**.

**disclosure**

The act of making known or revealing. Disclosure can also mean providing access to records or personal information.

**disclosure for audit purposes\***

Disclosure for the purposes of carrying out a financial or other formal and systematic examination or review of a program, portion of a program or activity that includes personal information about individuals, provided such examination or review is sanctioned by statute, regulation or public policy relating to the public body.

**discretion**

The power to make a decision that cannot be determined to be right or wrong in an objective sense. Discretion amounts to the power of the decision-maker to choose a particular course of action for good reasons and in good faith, after considering the relevant facts and circumstances; the applicable law, including the objects of the *FOIP Act*; and the proper application of the law to the relevant facts and circumstances.

**discretionary benefit**

A favourable or helpful factor, circumstance or advantage which may be granted to a person by a decision-maker who has the power to choose whether or how to grant it.

<b>discretionary exception</b>	Within the context of <b>Part 1</b> of the Act, an exception to disclosure that permits a public body to choose whether or not to withhold all or part of a record. Discretionary exceptions begin with the phrase “the head of a public body may refuse to disclose.” <i>See also</i> <b>mandatory exception</b> .
<b>educational body*</b>	A local public body that is <ul style="list-style-type: none"><li>• a university, technical institute or public college, as defined in the <i>Post-secondary Learning Act</i>;</li><li>• The Banff Centre as defined in the <i>Post-secondary Learning Act</i>; or</li><li>• a board, charter school or Regional authority as defined in the <i>School Act</i>.</li></ul> <i>See also</i> <b>local public body</b> .
<b>employee*</b>	Includes, in relation to a public body, a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body.
<b>enactment*</b>	An Act or a regulation or any portion of an Act or regulation. An “enactment of Alberta,” as defined in the FOIP Regulation, includes a Treasury Board directive.
<b>exceptions to disclosure</b>	Provisions of the Act which either require or permit a public body to withhold all or part of a record or personal information in the custody or under the control of a public body. The Act establishes limited and specific exceptions to the right of access where disclosure would reveal certain categories of information or would result in harm to the Government of Alberta, the public body or a third party. These exceptions, which are either mandatory or discretionary, are set out in <b>sections 16 to 29</b> of the Act.
<b>explicitly in confidence</b>	<i>See in confidence</i> .
<b>extension</b>	In the context of the access request process under the Act, the lengthening of the 30-day time limit for responding to the request. An extension can be claimed only if <ul style="list-style-type: none"><li>• the applicant does not provide enough details to enable the record to be identified;</li><li>• a large number of records are requested or must be searched and responding within 30 days would unreasonably interfere with the operations of the public body;</li><li>• more time is needed to consult with a third party or another public body before deciding whether to grant access to a record;</li><li>• a third party requests a review of the public body’s decision on access to third party information; or</li><li>• there are multiple concurrent requests made by the same applicant, or by two or more applicants who work for the same organization or who work in association with each other (the Commissioner has to approve extensions in these cases).</li></ul>
<b>fees</b>	The charges that an applicant pays to a public body for services related to the processing of an access request. The FOIP Regulation sets out the services for which fees may be charged and the maximum charges for providing these services. Fees may not exceed the actual cost of providing the service.
<b>financial information</b>	Information regarding the monetary resources of a third party, such as the third party’s financial capabilities, and assets and liabilities, past or present. Financial information is not limited to information relating to financial transactions in which the third party is involved. <i>See also</i> <b>commercial information</b> .

<b>FOIP</b>	The official abbreviation for “Freedom of Information and Protection of Privacy.”
<b>FOIP Coordinator</b>	<p>The position within a public body responsible for the overall management of its access to information and protection of privacy functions and responsibilities. The responsibilities of the FOIP Coordinator may include</p> <ul style="list-style-type: none"> <li>• managing the FOIP request process for the public body;</li> <li>• setting up practices and procedures to ensure that privacy protection measures are implemented within the public body;</li> <li>• coordinating any negotiations, mediations, inquiries, investigations and audits with the Office of the Information and Privacy Commissioner;</li> <li>• reporting as required to the Minister responsible for the <i>FOIP Act</i> on the operation of the Act; and</li> <li>• providing training and advisory services for the public body.</li> </ul>
<b>for</b>	In the context of the Act’s exclusions, “for” means on behalf of someone else, and is comparable to the word “by.” That is, a record “created by or for” a person is a record created by that person or by a person acting on his or her behalf. The fact that one person is acting for another must be evident in the record itself or in some other way.
<b>guardian</b>	<p>A guardian of a minor may exercise any right or power under the Act if the exercise of that right would not be an unreasonable invasion of the minor’s privacy. In most cases, parents are automatically the guardians of their children. Each guardian may exercise all the powers independently of the other, unless there is an agreement or court order to the contrary.</p> <p>A guardian or trustee of an adult with impaired capacity to make decisions may exercise the rights of that adult if the right of the adult that is being exercised is within the scope of the powers and duties set out in the guardianship or trusteeship document.</p>
<b>harm</b>	Damage or detriment. Within the context of the Act’s exceptions to disclosure, “harm” is the term used to refer to the injury to a particular public or private interest that could occur as the result of the disclosure of certain types of information in records in the custody or under the control of a public body. The harm must be specific to the context of the request. The general test for harm under the Act is whether there is a reasonable expectation of harm flowing from disclosure of the specific information at issue.
<b>harm(s) test</b>	<p>A test or set of criteria used to determine whether disclosure of records or information would cause damage or detriment to a particular interest. To meet the standard of proof required to decide that disclosure could reasonably be expected to cause harm, and therefore that a particular exception in the Act applies,</p> <ul style="list-style-type: none"> <li>• there must be a reasonable expectation of probable harm (not just a well-intentioned but unjustifiably cautious approach to the avoidance of any risk whatsoever because of the sensitivity of the matters at issue);</li> <li>• the harm must constitute damage or detriment, not mere interference or inconvenience; and</li> <li>• there must be a causal connection between disclosure and the anticipated harm.</li> </ul>
<b>head*</b>	<p>In relation to a public body, means:</p> <ul style="list-style-type: none"> <li>• for a department, branch or office of the Government of Alberta, the member of the Executive Council who presides over it;</li> </ul>



- if the public body is one designated in the FOIP Regulation, the person designated by the member of the Executive Council responsible for that body to act as the head of that body or, if a head is not so designated, the person who acts as the chief officer and is charged with the administration and operation of that body;
- for a local public body, the person or group of persons designated as the head by bylaw, or other legal instrument by which the local public body acts; and
- for any other case, the chief officer of the public body.

The head of a public body is the person or group of persons responsible for the administration of the *FOIP Act* within that public body.

**health care  
body\***

A local public body that is

- the board of an approved hospital, as defined in the *Hospitals Act*, other than one that is owned or operated by a regional health authority;
- the operator of a nursing home, as defined in the *Nursing Homes Act*, other than one that is owned and operated by a regional health authority;
- a provincial health board established under the *Regional Health Authorities Act*;
- a regional health authority under the *Regional Health Authorities Act*;
- a community health council established under the *Regional Health Authorities Act*; or
- a subsidiary health corporation as defined in the *Regional Health Authorities Act*.

See also **local public body**.

**implicitly  
in confidence**

A phrase applied to information that is furnished on the understanding of both parties that it be kept secret. There may be no actual statement of confidentiality, written agreement or other physical evidence of the understanding that the information will be kept confidential. Some of the relevant facts and circumstances that may show an understanding of confidentiality are how the information was provided, for what purpose, and how it was managed, secured or distributed by or within the public body.

**in camera**

In the absence of the public at large. A meeting of a local public body that is open to the public or to which the public at large is invited, even if no members of the public attend, is not a meeting held *in camera*.

**in confidence**

A term applied to information that is furnished with the intent that it be kept secret. In the context of the Act, the concept is applied to information or records supplied to a public body by third parties (including individuals and other levels of government) or by confidential sources of law enforcement information.

Whether information has been supplied explicitly or implicitly in confidence is a factor in considering exceptions to disclosure under **sections 16, 17, 18(3), 19, 20(1)(d) and 21(1)(b)**. The information must have been supplied in the expectation that the public body would not disclose it. The intention that the confidence will be maintained may be explicitly stated within the record in question or may be implied by the circumstances under which the information was submitted and received. Where confidentiality is implied, there must be objective grounds to support the assumption of confidentiality. See also **implicitly in confidence**.

**inquiry**

A process used by the Commissioner to conduct a review requested under the Act. If a review is not resolved in mediation, an inquiry may be conducted through written submissions or through oral presentations, which may be open to the public. In

conducting an inquiry, the Commissioner has all the powers provided under the *Public Inquiries Act* and under **section 56(2)** of the *FOIP Act*.

**intervenor**

A person, group or organization that does not have status under the Act (e.g. as an applicant or a public body) but has an interest in an issue being decided at an inquiry and is invited by the Commissioner to make a submission or present evidence.

**investigation**

A systematic process of examination, inquiry and observation. The Act's definition of "law enforcement," includes police, security and administrative investigations, including the complaint that leads to the investigation. Within this context, an investigation may be carried out by or on behalf of a public body or by a police service.

The term "investigation" also refers to the procedures used by the Commissioner to ensure compliance with the Act. After conducting an investigation, the Office of the Information and Privacy Commissioner may issue an Investigation Report or a letter of findings.

**judicial administration record\***

A record containing information relating to a judge of the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, or the Provincial Court of Alberta, or to a master of the Court of Queen's Bench of Alberta or a sitting justice of the peace or a presiding Justice of the Peace under the *Justice of the Peace Act*, including

- the scheduling of judges and trials;
- the content of judicial training programs;
- statistics of judicial activity prepared by or for a judge; and
- a record of the Judicial Council established under the *Judicature Act*.

**judicial review**

The power of the Court of Queen's Bench to determine whether the Commissioner has acted strictly within the powers that have been given to him or her. Such a review is not an appeal. It does not normally allow the court to substitute its decision for that of the Commissioner. A party to an inquiry by the Commissioner may apply for judicial review on jurisdictional grounds or on the basis of an error in law.

**labour relations information**

Relates to the management of personnel by a person or organization, whether or not the personnel are organized into bargaining units. It includes relationships within and between workers, working groups and their organizations as well as managers, employers and their organizations. Labour relations information also includes collective relations between a public body and its employees. Common examples of labour relations information are hourly wage rates, personnel contract and information on negotiations regarding collective agreements.

**law enforcement\***

For the purposes of both the access and privacy provisions of the Act, refers to

- policing, including criminal intelligence operations;
- a police, security or administrative investigation, including the complaint that gave rise to the investigation, that leads or could lead to a penalty or sanction being imposed. The penalty or sanction could either be imposed by the public body conducting the investigation or by another body to which the results of the investigation are referred; or
- proceedings that lead or could lead to a penalty or sanction being imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred.

**legal privilege**

There are several kinds of legal privilege. They include

- solicitor–client privilege;
- litigation privilege;
- common interest privilege;
- parliamentary privilege;
- police informer privilege;
- case-by-case privilege for private records and for Crown records; and
- statutory privilege.

*See also* **solicitor–client privilege**.

**legal proceedings**

Proceedings governed by rules of court or rules of judicial or quasi-judicial tribunals that can result in a judgment of a court or a ruling by a tribunal. Legal proceedings include all proceedings authorized or sanctioned by law, and brought or instituted in a court or legal tribunal, for the acquiring of a right or the enforcement of a remedy.

**licence or permit**

Authorization to carry out an activity, such as operating a particular establishment, or carrying on a professional or commercial activity. Examples include business licences, teaching permits, taxi licences, and building and development permits.

**local government body\***

A local public body that is

- a municipality, improvement district or regional services commission under the *Municipal Government Act*;
- a special area as defined in the *Special Areas Act*;
- a board established under the *Drainage Districts Act*;
- a board established under the *Irrigation Districts Act*;
- a housing management body established under the *Alberta Housing Act*;
- a Metis settlement or the Metis Settlements General Council established under the *Metis Settlements Act*;
- a police commission, police service or policing committee as defined in the *Police Act*;
- a municipal library board, library system board, federation board or joint municipal library board continued or established under the *Libraries Act*; or
- a board, committee, commission, panel, agency or corporation created or owned by a body referred to above and all of the members or officers of which are appointed or chosen by that body, but does not include EPCOR Utilities Inc. or ENMAX Corporation or any of their respective subsidiaries that own a gas utility, as defined in the *Gas Utilities Act*, that own a generating unit, transmission facility or electric distribution system as defined in the *Electric Utilities Act*, or whose primary business activity consists of providing electricity services as defined in the *Electric Utilities Act*.

**local public body\***

A public body that is an educational body, a health care body or a local government body. *See also* **educational body**, **health care body** and **local government body**.

**management of personnel**

Refers to aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees. For the Government of Alberta, the term includes the government-wide network managed through Corporate Human Resources. It does not include management of consultant, professional or other personal services contracts. *See also* **administration of personnel**.

<b>mandatory exception</b>	Within the context of <b>Part 1</b> of the Act, an exception to disclosure that requires a public body to withhold all or part of a record. Mandatory exceptions begin with the phrase “the head of a public body must refuse to disclose.” The mandatory exceptions are: <b>sections 16(1), 16(2), 17, 20(4), 22, 24(2.1) and 27(2)</b> . <i>See also discretionary exception.</i>
<b>mediation</b>	The process of facilitating discussion between parties with the goal of negotiating a mutually accepted resolution of the dispute.
<b>meeting*</b>	For the purposes of the Act’s exception for local public body confidences, means a meeting in its entirety or a portion of a meeting.
<b>Minister responsible for the Act</b>	The member of the Executive Council charged by the Lieutenant Governor in Council with the administration of the Act. The Minister responsible for the Act is the Minister of Service Alberta.
<b>non-arm’s length transaction</b>	<p>For the purposes of the Act’s exclusion for records of a treasury branch other than a record that relates to a non-arm’s length transaction between the Government of Alberta and another party, any transaction that has been approved by</p> <ul style="list-style-type: none"> <li>• the Executive Council or any of its committees;</li> <li>• the Treasury Board or any of its committees; or</li> <li>• a member of the Executive Council.</li> </ul> <p>This definition does not apply within the context of the Act’s exception to disclosure for third party business information. For the purposes of this exception, an “arm’s length transaction” is a transaction where the parties involved are unrelated, independent and acting in their own self-interest.</p>
<b>not contrary to the public interest</b>	<i>See public interest.</i>
<b>notice</b>	<p>An official communication required to be delivered to a member of the public, an affected third party, or an applicant in particular circumstances under the Act. Notice must be provided</p> <ul style="list-style-type: none"> <li>• to an affected third party where there is an intention to provide access to information which might be withheld under the Act’s exceptions for business information or personal privacy;</li> <li>• to an applicant, when the requested information might be withheld under the exceptions for business information or personal privacy and the third party has been notified;</li> <li>• to both the applicant and third party, to inform them of the decision on disclosure or non-disclosure of the third party’s information;</li> <li>• to the person concerned when his or her personal information is disclosed to an applicant because there are compelling reasons of health or safety to do so;</li> <li>• to an applicant when his or her request is transferred to another public body; and</li> <li>• to a third party whose information is disclosed in the public interest.</li> </ul>
<b>offence*</b>	Means an offence under an enactment of Alberta or Canada, including an offence under the <i>FOIP Act</i> .
<b>Officer of the Legislature*</b>	The Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, or the Information and Privacy Commissioner.

<b>Order</b>	A direction or decision issued by the Commissioner to conclude an inquiry.
<b>paramountcy</b>	<p>In the context of the Act's provision for the relationship between Acts, the concept of "paramountcy" provides the means for</p> <ul style="list-style-type: none"><li>• resolving a conflict or inconsistency between a provision of the <i>FOIP Act</i> and a provision of another enactment of Alberta, where neither the other Act nor the FOIP Regulation says that the other provision prevails despite the <i>FOIP Act</i>, or</li><li>• applying a provision in another Act or the FOIP Regulation that says that a provision of another enactment prevails despite the <i>FOIP Act</i>.</li></ul> <p>Where there is a conflict or inconsistency between the <i>FOIP Act</i> and a federal law, the doctrine of federal paramountcy applies. Under this doctrine, the federal law prevails over the provincial law, to the extent of the inconsistency.</p>
<b>peace officer</b>	A person employed for the purposes of preserving and maintaining the public peace (as defined in the <i>Police Act</i> ).
<b>penalty or sanction</b>	Includes a fine, imprisonment, and revocation of a licence or an order to cease an activity. For the purposes of the Act's exception for law enforcement, the penalty or sanction must be imposed under an enactment.
<b>person</b>	Within the context of the Act, a "person" means a "legal person," which includes an individual, a corporation, or any other entity.
<b>personal information*</b>	<p>Recorded information about an identifiable individual, including, but not limited to:</p> <ul style="list-style-type: none"><li>• the individual's name, home or business address, or home or business telephone number;</li><li>• the individual's race, national or ethnic origin, colour, or religious or political beliefs, or associations;</li><li>• the individual's age, sex, marital status or family status;</li><li>• an identifying number, symbol or other particular assigned to the individual;</li><li>• the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;</li><li>• information about the individual's health and health care history, including information about a physical or mental disability;</li><li>• information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;</li><li>• anyone else's opinion about the individual; and</li><li>• the individual's personal views or opinions, except if they are about someone else.</li></ul>
<b>personal information bank*</b>	A collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.
<b>personal representative</b>	A person who has the authority to administer a deceased individual's estate (e.g. an executor named in a will or a person with Letters of Administration from a court).
<b>policing</b>	Refers to the activities of police services. "Policing" means activities carried out under the authority of a statute regarding the maintenance of public order, detection and prevention of crime or enforcement of law.



<b>prescribed*</b>	Within the Act, means prescribed <i>by regulation</i> . For example, where the Act allows for use or disclosure of personal information where the individual concerned has provided consent “in the prescribed manner” the consent must meet the requirements set out in the FOIP Regulation.
<b>presumption</b>	An inference or assumption that a fact exists, based on the known or proven existence of some other fact or group of facts. Most presumptions are rules of evidence calling for a certain result in a given case unless the adversely affected party overcomes the presumption with other evidence. For example, the Act’s exception for personal privacy sets out particular types of personal information the disclosure of which is “presumed” to be an unreasonable invasion of a third party’s personal privacy.
<b>privacy impact assessment</b>	A process that assists public bodies in reviewing the impact that a new program, administrative process or practice, information system or legislation may have on individual privacy.
<b>proceeding</b>	An action or submission to any court, judge or other body having authority, by law or by consent, to make decisions concerning a person’s rights. This includes administrative proceedings before agencies, boards and tribunals that lead or could lead to a penalty or sanction being imposed, including a penalty or sanction imposed by another body to which the results of the proceeding may be referred.
<b>proprietary interest</b>	For the purposes of the Act’s exception for disclosure harmful to the economic interests of a public body, “proprietary interest” refers to a public body’s rights to information. Examples of information in which a public body may have a proprietary interest are geographical information systems, maps and statistical data.
<b>public body*</b>	<p>For the purposes of the administration of the Act, “public body” means</p> <ul style="list-style-type: none"> <li>• a department, branch or office of the Government of Alberta;</li> <li>• an agency, board, commission, corporation, office or other body designated as a public body in the FOIP Regulation or by a FOIP (Ministerial) Regulation;</li> <li>• the office of a member of the Executive Council;</li> <li>• the Executive Council Office;</li> <li>• the Legislative Assembly Office;</li> <li>• the office of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, or the Information and Privacy Commissioner; or</li> <li>• a local public body;</li> </ul> <p>but does not include</p> <ul style="list-style-type: none"> <li>• the office of the Speaker of the Legislative Assembly and the office of a Member of the Legislative Assembly; or</li> <li>• the Court of Appeal of Alberta, the Court of Queen’s Bench of Alberta, the Surrogate Court of Alberta or the Provincial Court of Alberta.</li> </ul> <p>The Act applies to records in the custody or under the control of a public body, and each public body, through its head, has statutory duties with regard to access to information and protection of privacy. <i>See also local public body.</i></p>
<b>public event or activity</b>	For the purposes of the Act’s exception for personal privacy, a <i>public event or activity related to a public body</i> means something of importance that happens or takes place, a particular occupation or pursuit that is staged in public or is of a public nature, and is

connected with the public body's mandate and functions and organized or sponsored by the public body.

An event or activity would be considered public if it was open to the public in general, or to a section of the public. The event or activity may be completely open and accessible to the public without charge, or access may be restricted because of the nature of the event or activity, for example, through ticket sales.

The fact that an event or activity that took place on the premises of a public body was observable by a member of the public does not make it a public event or activity.

**public interest**

For the purposes of the Act's mandatory provision for disclosure in the public interest, information "clearly in the public interest" refers to information of compelling public interest, not just of interest or of curiosity to the public, a group of people, a person or the applicant.

This is to be distinguished from the meaning of "public interest" in the context of the Act's provision for excusing fees. In this context, the measure of public interest is whether the information is likely to contribute significantly to public understanding of the operations or activities of a public body or is of major interest to the public in terms of environmental protection or protection of public health or public safety.

In the context of the Act's exception for personal privacy, the phrase "not contrary to the public interest" may be understood as not inconsistent with long-term community values, or with the good of society at large. A public body is not required to find that a disclosure *promotes* a public interest simply that disclosure is *not contrary to* the public interest. A public body may decide that a disclosure would be contrary to the public interest on the basis of its knowledge of risks to its clientele or the nature of the request (e.g. if the requested information could be used to commit a criminal act or harm an individual or property, then it is likely to be contrary to the public interest to disclose the information).

**quality  
assurance  
committee**

A committee whose purpose is to study, assess and evaluate the provision of health services with a view to continuous improvement of the quality of health care or health services, or the level of skill, knowledge and competence of health service providers. This term applies only to quality assurance committees as defined in the *Alberta Evidence Act* and not to other quality assurance committees established within either health care bodies or other public bodies to monitor the quality of health services or other services.

**reasonable**

Fair, proper, just, moderate, suitable under the circumstances. There are a variety of situations under the Act where reasonableness comes into play in a decision or course of action on the part of a public body, in particular,

- fulfilling the duty to assist applicants and to respond to requests without delay;
- deciding whether disclosure of personal information would constitute an unreasonable invasion of a third party's personal privacy;
- deciding whether disclosure of information that may be subject to certain exceptions under the Act could reasonably be expected to cause harm; and
- making certain determinations with respect to the collection, use, disclosure, and protection of personal information.

<b>reasonable expectation of harm</b>	In the context of certain exceptions in the Act, the phrase “reasonable expectation of harm” means that there is a clear cause-and-effect relationship between the disclosure and the harm; the disclosure will cause harm and not simply interference or inconvenience; and the likelihood of harm is genuine and conceivable.
<b>record*</b>	A record of information in any form. The term “record” includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner. The definition of “record” does not include software or any mechanism that produces records.
<b>records retention and disposition schedule</b>	A legal authority that describes the records under the control of a public body, specifies how long and where they must be kept as they progress through the phases of their life cycle, the format in which the records must be stored, and what their final disposition will be (destruction or archival preservation) at the end of their life cycle.
<b>request</b>	An application under the Act for access to records or personal information in the custody or under the control of a public body. <i>See also</i> <b>continuing request</b> .
<b>responsive records or information</b>	Any information or records that are reasonably related to an applicant’s access request. Responsiveness may be determined by analyzing the request and examining the records. The fact that an applicant already has or knows the substance of the information, or has knowledge of the contents of the records does not mean that the record can be considered non-responsive. A public body’s obligation is to address the applicant’s entire request.
<b>review</b>	In the context of the Act’s provisions for independent reviews of decisions made by public bodies, “review” refers to the examination by the Commissioner, or an adjudicator, of a decision, act or failure to act by the head of a public body in the course of processing a request for access to records or information under the Act. <i>See also</i> <b>inquiry</b> .
<b>routine disclosure</b>	A process whereby access to a record is granted without a request under the Act, usually in response to a routine inquiry or request. <i>See also</i> <b>active dissemination</b> .
<b>scientific information</b>	Information exhibiting the principles or methods of science. <i>See also</i> <b>technical information</b> .
<b>severing</b>	The physical removal, by masking or other means, of any information that is excepted from disclosure in order that the remainder may be disclosed.
<b>solicitor–client privilege</b>	This form of legal privilege applies to a record when <ul style="list-style-type: none"> <li>• the record is a communication between a lawyer and the lawyer’s client;</li> <li>• the communication entails the seeking or giving of legal advice; and</li> <li>• the record is intended to be confidential by the parties.</li> </ul>
<b>statistical survey</b>	Refers to general views or considerations of subjects using numerical data, such as a study of growth rates in various forested areas of northern Alberta.
<b>substance of deliberations</b>	For the purposes of the Act’s exceptions for Cabinet and Treasury Board confidences and local public body confidences, means the essence, material or essential part of the discussion or deliberation. “Deliberation” means the act of weighing and examining the reasons for and against a contemplated act or course of conduct or an examination of choices of direction or means to accomplish an objective.

<b>technical information</b>	Information relating to a particular subject, craft or technique, such as system design specifications and plans for an engineering project. <i>See also scientific information.</i>
<b>third party*</b>	Any person, group of persons or organization other than the person making a request (the applicant) or a public body. The term refers to a person, group of persons or organization whose information is in the custody or under the control of a public body and whose interests are affected by the public body's decision, as described in the Act's exceptions for third party business information and third party personal information of the Act.
<b>time limit</b>	The time allowed for a response to be made or an action to be taken. The <i>Alberta Interpretation Act</i> says that if a time is expressed to begin after or anything is to be done before a specified day, the time does not include that day. The 30-day time limit for processing requests is based upon calendar days, not working days. The time limit begins on the day after the request is received in a duly authorized office and any initial fee is paid. The 20-day time limit for a third party response begins on the day after the third party notice is given; and an applicant has 60 days from the day after being notified of a decision to request a review of that decision by the Commissioner. If a time limit expires on a Sunday or other holiday, the time limit is extended until the next working day.
<b>trade secret*</b>	<p>Information, including a formula, pattern, compilation, program, device, product, method, technique or process</p> <ul style="list-style-type: none"><li>• that is used, or may be used, in business or for any commercial purpose;</li><li>• that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use;</li><li>• that is the subject of reasonable efforts to prevent it from becoming generally known; and</li><li>• the disclosure of which would result in significant harm or undue financial loss or gain.</li></ul>
<b>transfer</b>	The act by which one public body formally passes to another public body responsibility for processing a request for access to, or correction of, records under the Act. A request may be transferred to another public body if the record was produced by or for the other public body; the other public body was the first to obtain the record; or the record is in the custody or under the control of the other public body.
<b>transitory record</b>	A record that has only immediate or short-term usefulness and will not be needed again in the future. Transitory records contain information that is not required to meet legal or financial obligations or to sustain administrative or operational functions, and has no archival value.







## APPENDIX 2

### DELEGATION AND ASSIGNMENT OF RESPONSIBILITY TABLES

#### 2.1 Delegation Table – Provisions of the *FOIP Act* and Regulation for which Delegation of Authority Should be Considered

Duty, power or function of Head	Section reference	Retained by Head	Delegated to FOIP Coordinator	Delegated to other person(s) (provide title(s) – specific or generic)
<b>Right of Access</b>				
Authority to declare request abandoned	8(1)			
Authority to grant continuing request	9(2)			
Duty to assist applicants	10(1)			
Duty to create records	10(2)			
Authority to decide on content of response/ grant or refuse access	11, 12(1)			
Authority to refuse to confirm or deny the existence of a record	12(2)			
Authority to decide how access will be given	13 Regulation 4			
Authority to extend time limit	14(1), (3)			
Authority to request Commissioner's permission for extension	14(1), (2)			
Authority to transfer a request for access	15			

<b>Duty, power or function of Head</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
<b>Exceptions</b>				
Authority to withhold information harmful to business interests of a third party	16			
Authority to withhold information harmful to personal privacy	17			
Authority to withhold information harmful to individual or public health or safety	18 Regulation 6(1), (3), (5)			
Authority to withhold confidential evaluations	19			
Authority to withhold information harmful to law enforcement	20			
Authority to withhold information harmful to intergovernmental relations	21			
Authority to withhold Cabinet confidences	22			
Authority to withhold local public body confidences	23			
Authority to withhold advice from officials	24(1)			
Authority to withhold information/records about audit by Chief Internal Auditor	24(2.1)			
Authority to withhold information harmful to economic interests of a public body	25			

<b>Duty, power or function of Head</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
Authority to withhold testing procedures, tests and audits	26			
Authority to withhold privileged information	27(1), (2)			
Authority to withhold information harmful to conservation of heritage sites or endangered species	28			
Authority to withhold information that is or will be available to public	29			
<b>Third Party Intervention</b>				
Duty to give third party notice	30			
Authority to decide whether to give access to third party information	31(1)			
Duty to give notice of decision	31(2)–(4)			
<b>Public Interest</b>				
Authority to disclose information in the public interest	32(1)			
Duty to give notice to third party, Commissioner	32(3), (4)			
<b>Collection, Correction, Protection of Personal Information</b>				
Authority to set aside collection requirements	34(3)			

<b>Duty, power or function of Head</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
Authority to decide on requests for correction of personal information	36(1)			
Duty to correct, annotate or link personal information, duty to notify previous recipients	36(3), (4)			
Duty to give notice to individual requesting correction	36(7)			
Authority to transfer a request for correction	37			
Duty to ensure protection of personal information	38			
<b>Use and Disclosure of Personal Information</b>				
Establishing rules for electronic consent	Regulation 7(5)(a)			
Establishing rules for oral consent	Regulation 7(6)(a)			
Authority to disclose to relative or adult interdependent partner of deceased individual	40(1)(cc)			
Authority to disclose to avert imminent danger to health or safety	40(1)(ee)			
Authority to approve conditions for disclosure for research and statistical purposes and for administration of research agreements	42(c)			
Authority to disclose to guardian of a minor	84(1)(e)			



<b>Duty, power or function of Head</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
<b>Reviews and Complaints</b>				
Authority to ask the Commissioner for advice	54(1)			
Authority to request Commissioner to disregard requests	55			
Authority to require Commissioner to examine original record on site	56(4)			
Right to make representations to the Commissioner	69(3), (5), (6)			
Duty to discharge burden of proof	71			
Duty to comply with Commissioner's Order	74			
<b>General Provisions</b>				
Duty to publish a directory of the body's personal information banks and keep it current	87.1(1), (4)			
Duty to record uses or disclosures of personal information not included in directory	87.1(3)			
Authority to specify categories of records available without formal request and require a fee	88			
Duty to make manuals available	89			

<b>Duty, power or function of Head</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
<b>Fees</b>				
Authority to assess and collect fees	93			
Authority to waive fees	93(4)			
Duty to give notice of decision to grant or refuse waiver request	93(4.1)			

## 2.2 Delegation Table – Administrative Responsibilities in the FOIP Act and Regulation that May be Assigned

Duty, power or function of public body	Section reference	Retained by Head	Delegated to FOIP Coordinator	Delegated to other person(s) (provide title(s) – specific or generic)
<b>Right of Access</b>				
Establishing process for receiving access requests	2(a), (c)			
Assuring process for access is made public	Regulation 3(1)			
<b>Collection, Accuracy and Retention of Personal Information</b>				
Establishing controls over the collection, use and disclosure of personal information	2(b)			
Authorizing routine correction of personal information	2(d)			
Ensuring authorized purpose of collection	33			
Assuring proper collection and notification	34			
Assuring accuracy of personal information	35(a)			
Applying retention standards	35(b)			
<b>Use and Disclosure of Personal Information</b>				
Assuring appropriate uses	39			
Assuring proper disclosures of personal information	40 (May be different for each provision)			
Disclosing in accordance with Part 1	40(1)(a)			

<b>Duty, power or function of public body</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
Disclosing if not an unreasonable invasion of third party's personal privacy	40(1)(b)			
Disclosing for original or consistent purpose	40(1)(c)			
Disclosing after individual consents	40(1)(d)			
Disclosing to comply with enactment of Alberta or Canada or treaty, arrangement or agreement made under enactment	40(1)(e)			
Signing personal information sharing agreements	40(1)(e)			
Disclosing in accordance with enactment of Alberta or Canada that authorizes or requires disclosure	40(1)(f)			
Disclosing to comply with subpoena, warrant or court order from court, person or body with jurisdiction in Alberta	40(1)(g)			
Disclosing where necessary for employee of public body or member of Executive Council to perform duties	40(1)(h)			
Disclosing where necessary for delivery of common or integrated program or service	40(1)(i)			

<b>Duty, power or function of public body</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
Disclosing to enforce legal right of Government of Alberta or public body	40(1)(j)			
Disclosing to collect debt or fine or make payment	40(1)(k)			
Disclosing to determine or verify eligibility for program or benefit	40(1)(l)			
Disclosing to Auditor General and other prescribed persons for audit purposes	40(1)(m)			
Disclosing to Member of Legislative Assembly to assist individual	40(1)(n)			
Disclosing to bargaining agent acting on behalf of employee	40(1)(o)			
Disclosing for archival purposes	40(1)(p)			
Disclosing to assist investigation	40(1)(q)			
Disclosing from one law enforcement agency to another law enforcement agency	40(1)(r)			
Disclosing to next of kin or friend of injured, ill or deceased individual	40(1)(s)			
Disclosing to expert under <b>section 18(2)</b> to protect individual or public safety	40(1)(u)			



<b>Duty, power or function of public body</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
Disclosing for legal proceedings to which Government of Alberta or public body is a party	40(1)(v)			
Disclosing through Minister of Justice and Attorney General to place of lawful detention	40(1)(w)			
Disclosing to manage or administer personnel	40(1)(x)			
Disclosing to enforce a maintenance order	40(1)(y)			
Disclosing to officer of the Legislature where necessary to carry out duties	40(1)(z)			
Disclosing for supervision of individual under control of correctional authority	40(1)(aa)			
Disclosing when information available to the public	40(1)(bb)			
Disclosing business contact information	40(1)(bb.1)			
Disclosing to lawyer acting for an inmate	40(1)(dd)			
Disclosing to administrator of <i>Motor Vehicle Accident Claims Act</i>	40(1)(ff)			
Post-secondary educational body only: disclosing alumni information for its own fund-raising activities and administering disclosure agreements	40(2)			

<b>Duty, power or function of public body</b>	<b>Section reference</b>	<b>Retained by Head</b>	<b>Delegated to FOIP Coordinator</b>	<b>Delegated to other person(s) (provide title(s) – specific or generic)</b>
Post-secondary educational body only: disclosing teaching and course evaluations	40(3)			
Disclosing for research and statistical purposes and for administration of research agreements	42, 43			









## APPENDIX 3

### MODEL LETTERS

#### Introduction

The following sample letters are provided to assist public bodies in corresponding with applicants, third parties and others in the processing of access requests. The sample letters are intended to provide general guidance and may be altered to suit the circumstances of each request.

The letters are as follows:

- A Acknowledgment of request
- A.1 Notice of processing an access request under the *Health Information Act*
- B Notification during a continuing request
- C Transfer of request
- D Notice regarding extension of time limit
- E Fee estimate
- F Abandonment of a request
- G Response to access request – Granting access
- H Response to access request – Access to all or part of record(s) refused
- I Response to access request – Record does not exist
- J Refusal to confirm or deny existence of a record
- K Letter to Speaker of the Legislative Assembly regarding parliamentary privilege
- L Notice to third party under section 30
- M Notice to applicant under section 30(5)
- N Notice to third party regarding decision under section 31
- O Notice to applicant regarding decision under section 31
- P Notice to third party under section 32 (disclosure in the public interest)
- Q Notice to third party under section 32 after disclosure of information
- R Notice to third party of disclosure of personal information under section 17(2)(b)
- S Acknowledgment of receipt of correction request
- S.1 Notice of processing a request for correction or amendment under the *Health Information Act*
- T Notification concerning a request for correction or annotation
- U Notice to public bodies regarding correction or annotation of personal information
- V Initial letter to expert under section 18(2)
- W Letter transmitting records to expert under section 18(2)

## Model Letter A – Acknowledgment of request

*Purpose: To acknowledge receipt of the applicant's request for information, to ask for clarification of a request and/or to request that initial fees be paid in order that the request may be considered complete and processing can commence.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*

[Request under Consideration]

Your request for access to [describe the information requested] under the *Freedom of Information and Protection of Privacy Act* (the Act) was received by [public body] on [date].

### Option A.1: General acknowledgment

We will provide the information available to you under the Act as quickly as possible. Although the Act allows us a maximum of 30 days to respond, we will reply sooner than [date], if possible.

### Option A.2: Need to supply more details

Unfortunately, your request for access to information does not provide sufficient specific details to identify the records you may be requesting. [Name of public body] cannot begin to process your request until we receive additional information to help us [identify the record *or* make the request more specific]. Please help us to clarify your request by supplying any of the following details of which you are aware:

[List details you are requesting]

### Option A.3: Failure to include initial fee

Unfortunately, you did not include the initial fee of \$25.00. The Act allows us 30 days to respond to your request, but this time period will not commence until the initial fee has been received. Please forward the fee to [appropriate address within the public body] as quickly as possible.

The processing of the request will commence immediately upon the receipt of your fee.

**Model Letter A – Acknowledgment of Request (continued)****Option A.4: Acceptance of continuing request**

We note that you wish your request to have continuing status under section 9 of the Act. [Name of public body] is granting the request continuing status, and a schedule indicating the period of the request and on what dates the continuing request will be deemed to be received and activated is attached. You will be notified on each of these dates that the request process has begun and when a response can be anticipated.

If you find this schedule unsatisfactory, please write to me or call me at [telephone number].

**Option A.5: Rejection of continuing request**

We note that you wish your request to have continuing status under section 9 of the Act. [Name of public body] does not grant your request [state reasons]. For these reasons, we will only respond to this request as a single access request for records that currently exist.

**Option A.6: Clarification of request**

We have now had an opportunity to discuss your request with you [state method and date]. We agreed that the request would now focus on [describe the subject and/or the information agreed upon]. If this understanding is not correct, please contact me at [telephone number] as soon as possible. This letter serves as a notice that it is this request that [name of public body] is proceeding to process. We will provide the information available to you under the Act as quickly as possible. Although the Act allows us a maximum of 30 days to respond, we will reply sooner than [date], if possible.

If you have any questions, please write to me or call me at [telephone number].

## **Model Letter A – Acknowledgment of Request (continued)**

### **Conclusion for options A.3 to A.6**

Section 65 of the *Freedom of Information and Protection of Privacy Act* provides that you may make a written request to the Information and Privacy Commissioner to review this matter. You have 60 days from the date of this notice to request a review by writing to the Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number noted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request form that you sent to [name of public body].

Sincerely,

[Name]

[Title]

**Model Letter A.1 – Notice of processing an access request under the Health Information Act**

*Purpose: To acknowledge receipt of the applicant's request for information, and to give notice that all or part of the request will be processed under the Health Information Act. **This model letter is only to be used by a public body that is also a custodian under the Health Information Act.***

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

Your request for access to [describe the information requested] under the *Freedom of Information and Protection of Privacy Act* was received by [public body] on [date].

Some [or all] of the record(s) you requested contain information to which the *Health Information Act (HIA)* applies. The request for these record(s) is deemed to be a request under section 8(1) of the *HIA* and that Act applies to the processing of your [or part of your] request.

Please see the attached letter related to your [or that part of your] request [attach a letter acknowledging receipt of the access request under the *HIA* – use Model Letter A from Appendix 2 – *Health Information Act Guidelines and Practices*].

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]

[Title]



## Model Letter B – Notification during a continuing request

*Purpose: To notify a requester who has made a continuing request that work has begun on processing records at a particular date set out in the schedule required by section 9 of the Act.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

### Option B.1: No fee required

[Name of public body] is commencing to process your continuing request concerning [set out general subject] in accordance with the established schedule. The processing, due to commence on [date], is now under way. We will make every effort to provide the information requested as quickly as possible and no later than [date].

### Option B.2: Deposit required

As indicated in the letter of [date of original fee estimate for the continuing request], [name of public body] will process your continuing request concerning [set out general subject] in accordance with the schedule established, when the deposit for this scheduled instalment of the request is received. Please forward the deposit of [\$ amount] made payable to [the Minister of Finance and Enterprise or appropriate officer of public body]. This reply must be sent to [name of officer, office and address of public body] and should quote the reference number provided at the top of this letter. When we have received your deposit, processing of your request will proceed.

If you have any questions now or during the processing of this portion of your request, please write or call me at [telephone number].

Sincerely,

[Name]  
[Title]

## Model Letter C – Transfer of request

*Purpose: To advise an applicant that his or her access request or request for correction of personal information has been transferred.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

Your request for [information or correction of your personal information] has been forwarded to [name of public body, address and telephone number] and this body has agreed to process it. Your request was transferred on [date] under [section 15 or 37] of the *Freedom of Information and Protection of Privacy Act* because [name of public body] [explain the reason for the transfer; i.e., the record was produced by or for the other public body or the other public body was the first to obtain the record, or the record is in the custody or under the control of the other public body].

[Name of the other public body] will respond to you before [date – 30 days from the date the other public body received the transferred request] unless it extends the time limit for responding to you under section 14. [Name of FOIP Coordinator] at [public body] will contact you shortly to acknowledge receipt of this request.

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]

[Title]

cc: [Other public body contact]

## **Model Letter D – Notice regarding extension of time limit**

*Purpose: To advise an applicant of a time extension taken to process a request.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

[Name of public body] received your request for access to information on [date].

Normally, [name of public body] responds to a request for information within 30 days after receiving the request. However, the *Freedom of Information and Protection of Privacy Act* provides that a public body may extend this time limit under certain circumstances.

### **Option D.1: Time extension to clarify request**

In this case, there is a need for us to obtain more information from you before we can identify the records that deal with the subject of your request. We will need a time extension of [number of days] to do this and identify the applicable records.

### **Option D.2: Consultation with third party or parties or other public body or bodies**

A preliminary review of the records you have requested indicates that extensive consultations with other parties including [name of third party or parties or public body or bodies] may be required before we can fully process your request. This consultation is necessary for us to deal completely with the records that are the subject of your request. We will require a time extension of [number of days] to carry out this process.

### **Option D.3: Large number of records**

Your request involves a large number of records. The volume of information involved cannot be processed within the usual 30-day limit. An extension of time of [number of days] will allow [name of public body] to provide you with a complete response to your request.

**Model Letter D – Notice regarding extension of time limit (continued)****Option D.4: Multiple concurrent requests**

[You or you and others working for the same organization or working in association with you] have made multiple concurrent requests. We have consulted with the Information and Privacy Commissioner about the difficulties this causes in terms of responding to all requests within the 30-day time limit in the Act. The Commissioner has given us permission to extend the time for responding by [number of days].

**Conclusion for all options**

A response to your request will be ready no later than [proposed date]. We will try to respond sooner, if possible.

If you have any questions regarding this time extension, please contact [name and job title] at [business address] or telephone [number].

If you feel this time extension is unjustified, section 65 of the *Freedom of Information and Protection of Privacy Act* provides that you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to request a review by writing to the Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request form that you sent to [name of public body].

Sincerely,

[Name]  
[Title]

## Model Letter E – Fee estimate

*Purpose: To advise an applicant of the amount of fees that will be involved in processing a request.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

[Name of public body] received your request for access to information on [date]. Section 93 of the *Freedom of Information and Protection of Privacy Act* provides that fees may be charged for providing you with the information that you requested.

Fees over and above the initial fee paid at the time you made the request are assessed because [provide rationale for fees being assessed].

The fee for providing the records you have requested is estimated to be [\$ amount]. We have calculated this amount as follows:

[Provide calculation]

### Option E.1: Deposit required

Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and enclose a deposit of [\$ amount] made payable to [the Minister of Finance and Enterprise or appropriate officer of public body]. This reply must be sent to [name of officer, office and address of public body] and should quote the reference number provided at the top of this letter. When we have received your response and deposit, processing of your request will continue.

### Option E.2: No deposit required

Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and will pay these fees when requested to do so. Please send the reply to [name of officer, offices and address of public body] and quote the reference number provided at the top of this letter. When we have received your response, processing of your request will continue.



**Model Letter E – Fee estimate (continued)****Option E.3: Refusal of fee waiver**

Your request for a fee waiver cannot be granted [state reason]. Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and enclose a deposit of [specify amount]. Please send the reply to [name of officer, offices and address of public body] and quote the reference number provided at the top of this letter. When we have received your response, your request will be processed.

If you find the fees a burden to you, we would be pleased to discuss approaches to processing the request that may reduce the fees and still provide the information you require. Please write or call [name, title, address and telephone number], who may be able to assist you.

**For options E.1 and E.2**

Section 93(4) provides some limited situations where fees can be reduced, or waived entirely, if you cannot afford to pay or there are other reasons that justify excusing the fee, or if the record relates to a matter of public interest. If you believe that one of these circumstances applies to you, you should raise it with the officer mentioned above.

[You may wish to include a copy of the relevant pages of *FOIP Guidelines and Practices* on the subject of fee waivers or the Bulletin on Fee Waivers.]

**Conclusion for all options**

If you have any questions, please write or call the officer named above or myself at [telephone number].

Section 65 of the *Freedom of Information and Protection of Privacy Act* allows you to ask the Information and Privacy Commissioner to review this fee estimate and any decision made on a request for a fee waiver. The Act allows you 60 days from the date you receive this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

**Model Letter E – Fee estimate (continued)**

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [name of public body].

Sincerely,

[Name]

[Title]

**Model Letter F – Abandonment of a request**

*Purpose: To inform the applicant that his or her request is going to be considered abandoned under section 8. The time line to allow the applicant to reactivate the request within 6 months is a suggested guideline, not a requirement of the Act. Public bodies may choose to alter this according to the nature of the request or the records involved.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

**Option F.1: Abandonment indicated**

You indicated to us on [date] that you were abandoning your request [reference number and subject]. If you wish to reactivate your request at any time up to [date 6 months from the date of closure], you may do so without making another request or submitting an initial fee. After that date, you will have to submit another request and any initial fee that may be required.

**Option F.2: Abandonment not indicated**

We have not received any communication concerning your request since [date of letter seeking further information or requesting fee]. For this reason, we are closing the file on your request [reference number and subject]. If you wish to reactivate your request at any time up to [date 6 months from the date of closure], you may do so without making another request or submitting an initial fee. After that date, you will have to submit another request and any initial fee that may be required.

If you have any questions, please write or call me at [telephone number].

If you disagree with this decision, section 65 of the *Freedom of Information and Protection of Privacy Act* provides that you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to request a review by writing to the Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

**Model Letter F – Abandonment of a request (continued)**

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter
3. A copy of your original request for information that you sent to [name of public body].

Sincerely,

[Name]

[Title]

**Model Letter G – Response to access request – Granting access**

*Purpose: To inform an applicant that access will be granted.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request Under Consideration]

I am responding to your request of [date] for access to information.

We are pleased to provide access to [specify subject and records generally].

**Option G.1: Copy attached**

A copy of the record is attached.

**Option G.2: Applicant to view originals**

You have requested an opportunity to examine the original records rather than receive copies of them. We invite you to examine the record(s) at [place and address] on [date] at [time]. If you are unable to examine the records at that time, please contact [name and telephone number] to make alternate arrangements.

**Option G.3: Records cannot be copied**

The record(s) you have requested cannot be copied because [provide reason]. We invite you to examine the original record(s) at [place and address] on [date] at [time]. If you are unable to examine the record(s) at that time, please contact [name and telephone number] to make alternate arrangements.

**Option G.4: Fees required**

As we informed you in our fee estimate of [date], your request has now been processed and fees totaling [\$ amount and calculation, if previous deposit received] must be paid before access can be provided.



### **Model Letter G – Response to access request – Granting access (continued)**

Please make your cheque or money order payable to [Minister of Finance and Enterprise or appropriate officer of local public body] and send it to [name of officer, office and address of public body].

If you feel that your request has not been answered completely or that you require further clarification, please contact [name and job title] at [business address and telephone number].

Under section 65 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the assessment of a fee or any other matter concerning this response to your request. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [name of public body].

Sincerely,

[Name]

[Title]

## Model Letter H – Response to access request – Access to all or part of records refused

*Purpose: To inform an applicant that access to all or part of the records requested has been refused.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

I am replying to your request of [date] for access to [general subject of records].

### Option H.1: Total denial

Unfortunately, access to all the information that you requested is refused under section(s) [put in an explanation, including the detailed sections on which refusal is based].

### Option H.2: Some records available

I am pleased to inform you that access is being provided to [specify particular records].

- A copy of the record(s) is attached; or
- You requested to examine the original records rather than receive copies. We invite you to examine the record(s) at [place and address] on [date] at [time]. If you are unable to examine the records at that time, please contact this office to make alternative arrangements; or
- The record(s) to which you are being given access cannot be copied. We invite you to examine the original record(s) at [place and address] on [date] at [time]. If you are unable to examine the record(s) at that time, please contact this office to make alternative arrangements.

Access to all other records has been denied under section(s) [give precise references] of the *Freedom of Information and Protection of Privacy Act*.

### Option H.3: Severed information

Some of the records you requested contain information that is withheld from disclosure under the *Freedom of Information and Protection of Privacy Act*. We have severed the excepted information so that we could disclose to you the remaining information in the records.

**Model Letter H – Response to access request – Access to all or part of record(s) refused (continued)**

The severed information is withheld from disclosure under sections [provide section numbers and descriptors] of the Act. The detailed sections supporting the excising of particular information are [provided in the attached list or indicated on the face of each record].

**Option H.4: Excluded records**

The following records that you requested [describe records] are excluded from the scope of the *Freedom of Information and Protection of Privacy Act* under section [provide paragraph of section 4]. Therefore, we are not disclosing these records to you.

OR

We are disclosing [all or part of the particular records] outside the provisions of the *Freedom of Information and Protection of Privacy Act* and a copy of these is attached.

[If fees are to be charged, reference should be made to the options for additional wording in Model Letter G.]

Under section 65 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the decision [not to disclose information that you requested] OR [that the records you requested are excluded from the scope of the Act]. You have 60 days from the receipt of this notice to request a review by writing the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [name of public body].

Sincerely,

[Name]  
[Title]

**Model Letter I – Response to access request – Record does not exist**

*Purpose: To advise an applicant that a record does not exist.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

I am writing about your request of [date] for access to information under the *Freedom of Information and Protection of Privacy Act*.

I regret to inform you that a search by [name of public body] has failed to retrieve any records relating to the subject of your request. [Outline all steps taken to locate records and, if the records have been destroyed, provide information, if possible, as to when and under what authority this was done.]

If you have any questions about this letter, please write or call me at [telephone number].

Under section 65 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the finding that records relevant to the request [could not be located or have been destroyed]. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [name of public body].

Sincerely,

[Name]

[Title]

## Model Letter J – Refusal to confirm or deny existence of a record

*Purpose: To respond to an applicant where it is necessary to "neither confirm nor deny" the existence of a record.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

I am writing about your request of [date] for access to information concerning [specify subject].

We are unable to confirm or deny the existence of the record(s) you have requested. However, if such information did exist, it would be withheld from disclosure under sections [specify sections and descriptors] of the *Freedom of Information and Protection of Privacy Act*.

If you have any questions about this decision, please write or call me at [telephone number].

Under section 65 of that Act, you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to ask for a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [name of public body].

Sincerely,

[Name]  
[Title]



**Model Letter K – Letter to Speaker of the Legislative Assembly regarding parliamentary privilege**

*Purpose: To obtain a determination from the Speaker of the Legislative Assembly as to whether or not records contain information subject to parliamentary privilege.*

[Reference number]

[Date]

[Speaker's name and address]

Dear [Name of Speaker]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

[Name of public body] has received a request under the *Freedom of Information and Protection of Privacy Act*. The request is for records concerning [subject of request] and we believe that the records attached to this letter may contain information that is subject to parliamentary privilege under section 27(1) of the Act.

I would appreciate your assistance in making a determination, as required under section 27(3) of the Act, as to whether or not parliamentary privilege applies in this case. We received the request on [date] and must respond to the applicant by [date]. Your prompt attention to this matter would also be most appreciated.

If you have any questions regarding the records or the request do not hesitate to call me at [telephone number].

Sincerely,

[Head of public body]  
[Title]

Attachment

### Model Letter L – Notice to third party under section 30

*Purpose: To advise a third party that an applicant has requested access to information that affects their business interests or personal privacy.*

[Reference number]

[Date]

[Third party's name]

Dear [Third party's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

[Name of public body] has received a request under the *Freedom of Information and Protection of Privacy Act* (the Act) to disclose [describe the records as they relate to the third party]. A copy of the information that pertains to you accompanies this letter [include a copy of the record whenever possible without disclosing information that is excepted under the Act].

[Make a note of the portion of the record that is being considered for severing, if that is the case.]

If you are not the appropriate party to receive this Notice, or if another third party may also have an interest in the information or be affected by the disclosure of the information, please notify me at the telephone number noted at the end of this letter.

We would appreciate receiving your views regarding disclosure of this information.

#### **Option L.1: Business interests (section 16)**

As section 16 of the Act indicates, [name of the public body] must disclose information to the applicant unless:

- the records contain certain types of information as described on the attached sheet; and
- the information was supplied in confidence; and
- the disclosure of the information could reasonably be expected to result in one or more of the harms specified on the attached sheet.

A public body must refuse to disclose information that was collected on a tax return, or collected for the purposes of determining tax liability or in collecting a tax.

A copy of section 16 of the Act is attached to this letter to assist you. After reviewing the material, please provide your views on the disclosure of the records in writing to [me, or name and job title] by [date]. You have 20 days in which to respond to this notice [insert the actual date when the response is due, if possible]. You may either: (1) consent to the disclosure of the information; or, (2) make written representations explaining why the information should not be disclosed.

**Model Letter L – Notice to third party under section 30 (continued)**

If you wish to have any of the information pertaining to your business withheld, it is important that you provide clear and specific reasons that focus on the type of harm that may result as specified in section 16 of the Act.

Your input and other relevant factors will be considered when deciding whether to disclose the requested information. Please note that, if we do not receive written representations from you by [date], we are required under the Act to make a decision based on the information that we have available. I will write to you by [date] to inform you of [public body's] decision.

**Option L.2: Personal privacy (section 17)**

As section 17 of the Act (attached) indicates, [name of the public body] is required to withhold personal information if it is determined that disclosure would be an unreasonable invasion of a third party's personal privacy.

Because disclosure of the requested records might be an unreasonable invasion of your personal privacy, your input would be valuable in helping us decide whether to disclose them.

You have 20 days from the date on this notice to respond [insert actual date when response is due, if possible]. After reviewing the accompanying material, please write to [me, or name and job title] by [date] indicating whether you consent to the disclosure of the information or explaining why you feel the information should be withheld.

Your input and other relevant factors will be considered when deciding whether to disclose the requested information. Please note that, if we do not receive written representations from you by [date], we are required under the Act to make a decision based on the information that we have available. I will write to you by [date] to inform you of [public body's] decision.

For further information concerning your rights and responsibilities under the *Freedom of Information and Protection of Privacy Act*, please refer to the accompanying Explanatory Notes [either Third Party Notice re: Business Interests, or Third Party Notice re: Personal Information].

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]

[Title]

## **Model Letter L – Notice to third party under section 30 (continued)**

### **Explanatory Note**

#### **Notice under Section 16 Third Party Business Interests**

The *Freedom of Information and Protection of Privacy Act* provides a right of access to records held by public bodies.

We have received a request for access to records in which you have an interest. We are required to provide access to as much of the requested records as possible. We may withhold only the information covered specifically in the Act's exceptions.

We are notifying you in order to give you an opportunity to express any concerns that you may have about disclosure of the records. To be withheld from disclosure, the third party business information must meet *all three* of the criteria in section 16 of the Act, harm to the business interests of a third party.

These criteria are:

1. The information is a trade secret or commercial, financial, labour relations, scientific or technical information of a third party.
2. The information was supplied, implicitly or explicitly, in confidence. There must be evidence that the information has been consistently treated in a confidential manner.
3. One or more specified harms will occur if the information is disclosed. The disclosure of the information will:
  - harm significantly the competitive position or interfere significantly with the contractual or other negotiations of the third party;
  - result in similar information no longer being supplied to the public body where it is in the public interest that similar information continues to be supplied (this does not apply where a statute or regulation requires that the information be supplied);
  - result in undue financial loss or gain to any person or organization; or
  - reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer, or other person or body appointed to resolve or inquire into a labour dispute.

**Model Letter L – Notice to third party under section 30 (continued)****Explanatory Note (continued)****Notice under Section 16  
Third Party Business Interests**

A public body must refuse to disclose any information about a third party that was collected on a tax return or collected for the purpose of determining tax liability or collecting a tax.

You have two options:

1. You may consent in writing to the disclosure of all or some of the information; or
2. If you feel that the provisions in section 16 apply to some or all of the information in the requested records, you may make written representations to us. Your representations should be directed only to information you would like to have withheld from disclosure. It must provide detailed evidence to support your claim for the exception. Please mark the exact portions of the records you wish to have withheld.

Your representations will be one of the factors that we consider in deciding whether or not to disclose all or part of the records. If we decide to disclose all or part of the records, you will be notified beforehand. If you disagree with the decision, you may ask the Information and Privacy Commissioner to review the decision.

For further information, please contact [name of coordinator, name of public body, address, telephone and fax numbers].



## **Model Letter L – Notice to third party under section 30 (continued)**

### **Explanatory Note**

#### **Third Party Notice under Section 17 Protection of Personal Privacy**

*The Freedom of Information and Protection of Personal Privacy Act* balances the public's right of access to records with the need to protect the privacy of individuals whose personal information is held by public bodies.

We have received a request under the Act by another person or organization for access to your personal information. We are notifying you in order to give you an opportunity to express any concerns that you may have regarding the disclosure of the personal information.

You have two options:

1. You may consent in writing to the disclosure of some or all of the information; or
2. You may make tell us, in writing, your concerns about the disclosure of the information, and explain why it would be an unjustified invasion of your privacy.

We will consider your representations in deciding whether or not to disclose the requested personal information. If it is decided that some or all of the information is to be disclosed, we will notify you before this takes place. If you disagree with that decision, you may ask the Information and Privacy Commissioner to review the decision.

For further information, please contact [name of coordinator, name of public body, address, telephone and fax numbers].

**Model Letter M – Notice to applicant under section 30(5)**

*Purpose: To advise an applicant that a third party will be consulted about disclosure of the requested information.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

On [date], I received your request for access to records held by [name of public body].

The requested records contain information that, if disclosed, may affect the interests of another person or organization. We have contacted the affected party, as required under section 30 of the Act, to provide them with an opportunity to consent to disclosure or to make representations explaining why disclosure would be [an unreasonable invasion of their personal privacy or may harm their business interests]. We will notify you of our decision regarding your request by [date].

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]

[Title]

## Model Letter N – Notice to third party regarding decision under section 31

*Purpose: To advise a third party of decision on disclosure.*

[Reference number]

[Date]

[Third party's name and address]

Dear [Third party's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

### **Option N.1: Third party representations received objecting to disclosure; public body decides to refuse access to the records**

Thank you for your views on the disclosure of [describe requested records as they relate to the third party].

After considering your representations in favour of refusing disclosure of these records, [name of public body] has decided to refuse the applicant's access request. This decision is based on [insert specific sections of the Act and the reasons those sections apply].

Upon notification of our decision, the applicant has 60 days to ask for a review by the Information and Privacy Commissioner. If that happens, the Commissioner may contact you as an interested party.

### **Option N.2: Third party representations received objecting to disclosure; public body decides to give access to all or part of the records**

Thank you for your views on the disclosure of [describe requested records as they relate to the third party].

After considering your representations in favour of refusing disclosure of these records and other relevant factors, [name of public body] has decided to give the applicant access to the records [or access to the records subject to exceptions permitted or required under the Act]. [If access is subject to exceptions, describe the parts of the records that will be disclosed and the parts that will be withheld. Provide copies or insert specific sections of the Act under which information will be withheld, and the reasons the sections apply. If full access, insert explanation of why sections 16 or 17 do not apply to the information that was the subject of the third party's representations.] This decision is based on [insert specific sections of the Act and the reasons those sections apply].

You may ask the Information and Privacy Commissioner to review the decision to disclose these records. You have 20 days from the date of this notice to request a review by writing the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

**Model Letter N – Notice to third party regarding decision under section 31  
(continued)**

If no request for a review is made within 20 days, the applicant will be given access to the records.

**Option N.3: Third party consented to disclosure of information; public body decides to refuse access to the records because another exception applies**

Thank you for your views on the disclosure of [describe requested records as they relate to the third party].

After considering all the relevant factors, [name of public body] has decided to refuse the applicant access to these records. The decision is based on [insert specific sections of the Act under which information will be withheld, and the reasons the sections apply – *note that information cannot be withheld under sections 16 or 17 if the third party that is involved has consented to disclosure; however, another exception may apply.*]

This decision was made by [name and job title].

Upon receipt of the response to this request, the applicant has 60 days to ask the Information and Privacy Commissioner to review this decision.

**Option N.4: Third party consented to disclosure; public body decides to give access to all or part of the records**

Thank you for your views on the disclosure of [describe requested records as they relate to the third party].

[Name of public body] has decided to give the applicant access to these records [or access to these records subject to exceptions permitted or required under the Act]. [If access is subject to exceptions, provide copies or describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply – *note that information cannot be withheld under sections 16 or 17 if the affected third party has consented to disclosure; however, another exception may apply.*]

This decision was made by [name and job title].

[Insert this paragraph if the applicant will be given access subject to exceptions.] After receiving these records, the applicant has 60 days to ask for a review by the Information and Privacy Commissioner.

**Option N.5: No response received from third party; public body decides to refuse access to the records**

We have not received your reply to our letter of [date of third party notice] which requested your views on disclosure of [describe records as they relate to the third party]. [Name of the public body] has decided to refuse the applicant access to these records. This decision is based on [insert specific sections of the Act and the reasons those sections apply].

**Model Letter N – Notice to third party regarding decision under section 31  
(continued)**

This decision was made by [name and job title].

The applicant has 60 days to ask the Information and Privacy Commissioner to review this decision. If that occurs, the Commissioner may contact you as an interested party.

**Option N.6: No response received from third party; public body decides to give access to all or part of the records**

We have not received your reply to our letter of [date of third party notice], which requested your views on disclosure of [describe records as they relate to the third party]. [Name of the public body] has decided to give the applicant access to these records [or access to these records subject to exceptions permitted or required under the Act]. [If access subject to exceptions is given, provide a copy or describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply.]

This decision was made by [name and job title].

**Conclusion for Options N.2 and N.6**

Under section 65 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the decision to disclose these records. You have 20 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

If no request for review is made within 20 days [insert final date for requesting a review, if possible], we will give the applicant access to the records. If you have any questions, please write to me or call me at [telephone number].

[Insert the following paragraph if applicant will be given access subject to exceptions.] The applicant has the right to ask the Information and Privacy Commissioner to review the decision to deny access to a part of the records.

Sincerely,

[Name]

[Title]



**Model Letter O – Notice to applicant regarding decision under section 31**

*Purpose: To advise an applicant of a decision regarding disclosure under the third party notification process.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request under Consideration]

**Option O.1: Third party representations received objecting to disclosure and public body decides to refuse access to the records**

We have reached a decision about your request of [date] for access under the *Freedom of Information and Protection of Privacy Act* to [briefly state subject of records requested].

After considering all relevant factors, including representations received from the third party whose interests could be affected by the disclosure of the records, we have refused access to the requested records based on [insert specific sections of the Act and the reasons those sections apply].

This decision was made by [name and job title].

**Option O.2: Third party representations received objecting to disclosure or no response received from third party and public body decides to give access to all or part of the record(s)**

I am writing about your request of [date] for access under the *Freedom of Information and Protection of Privacy Act* dealing with [subject of record(s)].

We have notified the affected third party and have given that party [those parties] an opportunity to make representations. [Name of public body] has decided to give access to the records you requested [or access to the records you requested, subject to exceptions permitted or required under the Act].

[If applicable] You should be aware that you will be required to pay [\$ amount] in fees before final access may be provided.

This decision was made by [name and job title].

The third party has 20 days to request that the Information and Privacy Commissioner reviews this decision. If the third party does not request the Commissioner to review this decision, we will give you access to the records on [date].

[For full access, insert the details of providing access.]

**Model Letter O – Notice to applicant regarding decision under section 31 (continued)**

[For access subject to exceptions, describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply. Provide access details.]

**Option O.3: Third party consents to disclosure of information; the public body decides to give access to all or part of the records**

I am writing about your request of [date] for access under the *Freedom of Information and Protection of Privacy Act* to [describe requested records].

The affected third party has consented to the disclosure of the information. I am pleased to advise you that [name of public body] has decided to provide access to the records you requested [or access to the records you requested, subject to exceptions permitted or required under the Act].

The decision was made by [name and job title].

[For full access, provide details of giving access.]

[For access subject to exceptions, describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply – *note that information cannot be withheld under sections 16 and 17 if the affected third party has consented to disclosure; however, another exception may apply.*]

**Option O.4: Third party consented to disclosure of information; public body decides to refuse access to the records under another exception**

I am writing about your request of [date] for access under the *Freedom of Information and Protection of Privacy Act* to [describe requested record(s)].

The affected third party has consented to the disclosure of the information. However, access to the requested record(s) is refused on the basis of [insert specific sections of the Act and the reasons those sections apply].

This decision was made by [name and job title].

**Model Letter O – Notice to applicant regarding decision under section 31 (continued)****Conclusion for all options**

Under section 65 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review [this decision] OR [this decision to deny access to the record(s)] OR [any aspect of this decision] OR [any decision to deny access to a part of these records]. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

[If the nature of the request warrants it, the public body may also wish to include the following paragraph.]

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

If you wish to request a review, please provide the Commissioner's office with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [name of public body].

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]

[Title]

**Model Letter P – Notice to third party under section 32 (disclosure in the public interest)**

*Purpose: To give a third party notice, before the fact, that information concerning the party will be disclosed through use of the public interest override.*

[Reference number]

[Date]

[Third party's name and address]

Dear [Third party's name]:

Re: Disclosure of Information in the Public Interest

Section 32 of the *Freedom of Information and Protection of Privacy Act* requires a public body to disclose information

1. about a risk of significant harm to the environment, to the health or safety of the public, a group of people or an individual; or
2. the disclosure of which is, for any other reason, clearly in the public interest.

In accordance with this requirement, [name of public body] intends to disclose information that relates to you, in the public interest. [Describe how the information relates to the third party. Explain why section 32 applies to the records in question. Provide a copy of the record if a record exists.]

We would appreciate receiving your views regarding disclosure of these records. Because of the urgency of the circumstances, I ask that you contact me [address, telephone and fax numbers] by [date and time] if you wish to make representations explaining why the records should not be disclosed.

Sincerely,

[Name]

[Title]

Attachment

**Model Letter Q – Notice to third party under section 32 after disclosure of information**

*Purpose: To advise a third party, after the fact, that information concerning the party has been disclosed under the public interest provision.*

[Reference number]

[Date]

[Third party's name and address]

Dear [Third party's name]:

Re: Notice of Disclosure of Information under the *Freedom of Information and Protection of Privacy Act*, section 32(4)

[Name of public body] has disclosed information that relates to you in compliance with the requirements of section 32 of the *Freedom of Information and Protection of Privacy Act*. This Act requires a public body to disclose information

1. about a risk of significant harm to the environment, to the health or safety of the public, a group of people, or an individual; or
2. the disclosure of which is, for any other reason, clearly in the public interest.

The information disclosed is [explain the information, provide a copy of the record if a record exists, and explain why section 32 applies to the information]. This decision was made by [name and job title].

Sincerely,

[Name]

[Title]

Attachment

cc: Information and Privacy Commissioner

**Model Letter R – Notice to third party of disclosure of personal information under section 17(2)(b)**

*Purpose: To advise an individual that personal information about him or her has been disclosed because there are compelling circumstances affecting someone's health or safety*

[Date]

[Third party's name and address]

Dear [Third party's name]:

Re: Disclosure of Information for Health or Safety

On [date], [Name of public body] disclosed personal information about you to [name of person and/or organization that received information]. The information consisted of [describe the information disclosed].

The information was disclosed in accordance with section 17(2) of the *Freedom of Information and Protection of Privacy Act*, which states that personal information may be disclosed if there are compelling circumstances affecting anyone's health or safety.

The Act requires that we notify you of this disclosure.

If you have any questions, please write to me or call at [telephone number].

Sincerely,

[Name]

[Title]



### Model Letter S – Acknowledgment of receipt of correction request

*Purpose: To acknowledge receipt of the applicant's request to correct his or her personal information.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request for Correction under Consideration]

Your request for correction of your personal information under the *Freedom of Information and Protection of Privacy Act* was received by [name of public body] on [date].

We will respond to your request by [date], or sooner if possible.

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]

[Title]

**Model Letter S.1 – Notice of processing a request for correction or amendment under the Health Information Act**

*Purpose: To acknowledge receipt of the applicant's request to correct his or her health information and to give notice that all or part of the request will be processed under the FOIP Act. This model letter is only to be used by a public body that is also a custodian under the Health Information Act.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request for Correction or Amendment under Consideration]

Your request for correction or amendment of information [describe requested correction or amendment] under the *Freedom of Information and Protection of Privacy Act* was received by [name of public body] on [date].

Some [or all] of the records you requested to be corrected or amended contain information to which the *Health Information Act (HIA)* applies. The request for correction or amendment of those records is deemed to be a request under section 13 of the *HIA* and that Act applies to the processing of your [or that part of your] request.

Please see the attached letter related to your [or that part of your] request [attach a letter acknowledging receipt of request for correction under the *HIA* – use Model Letter H from Appendix 2 – *Health Information Act Guidelines and Practices*].

If you have any questions, please write or call me at [telephone number].

Sincerely,

[Name]

[Title]

**Model Letter T – Notification concerning a request for correction or annotation**

*Purpose: To advise an individual whether or not a request for correction has been agreed to and, where it has not, that the record has been annotated.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: *Freedom of Information and Protection of Privacy Act*  
[Request for Correction under Consideration]

**Option T.1: Correction agreed to**

Your request for a correction of [error or omission] has been agreed to by [name of public body] and your record has been corrected as you requested.

A copy of your new record incorporating the correction accompanies this notice [or you can inspect the corrected record at – name and address of appropriate office].

**Option T.2: Correction refused**

Your request for a correction of [error or omission] has been refused by [name of public body], but [your record has been annotated recording the correction that you requested and the fact that it was not made OR the correction that you requested and the fact that it was not made has been linked to your record]. A copy of the completed form used to make the annotation is included with this notice. If you wish additional information to be included in the annotation, please provide it to us in writing.

The following public bodies, [name public bodies], to which the information has been disclosed over the last year have been informed of the facts of [the correction or annotation] and requested to amend their files to reflect this information.

[In the case of refusal] You may request the Information and Privacy Commissioner to review our decision to refuse to correct your personal information. The Act allows you 60 days from the date you receive this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

**Model Letter T – Notification concerning a request for correction or annotation  
(continued)**

*If the nature of the request warrants it, the public body may also wish to include the following paragraph:*

Section 67(1) of the *Freedom of Information and Protection of Privacy Act* requires the Commissioner to give a copy of your request for review to the head of a public body and to any other person who, in the Commissioner's opinion, is affected by the request. Therefore your request for review should not contain any information that you do not wish exchanged with the other parties.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for correction which you sent to [name of public body].

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]

[Title]

**Model Letter U – Notice to public bodies regarding correction or annotation of personal information**

*Purpose: To advise public bodies which have received personal information that a correction or annotation has been made.*

[Reference number]

[Date]

[Name of public body]

Dear [Name of official]:

On [date], [name of originating public body] disclosed to you information concerning [name of person requesting correction]. This information has been [corrected and a copy of the corrected record is attached, or annotated in the following way to reflect a correction requested but not made]. Section 36(4) of the *Freedom of Information and Protection of Privacy Act* requires that we notify you of this correction. Please amend your records or link the correction or annotation to them in order to ensure that they contain this new information.

Sincerely,

[Name]

[Title]

### Model Letter V – Initial letter to expert under section 18(2)

*Purpose: To establish conditions for the disclosure of personal information to an expert under section 18(2).*

[Reference number]

[Date]

[Name and address of expert]

Dear [Name of expert]:

Thank you for agreeing to help us make a determination concerning the disclosure of personal information under section 18(2) of the *Freedom of Information and Protection of Privacy Act*. This section provides that the head of a public body may refuse to disclose to an applicant personal information about the applicant if, in the opinion of a physician, a regulated member of the College of Alberta Psychologists, or a psychiatrist, or any other appropriate expert depending on the circumstances of the case, the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's health or safety.

As we have already discussed with you, we wish you to provide an expert opinion as to whether or not [specify general nature of records and health or safety issue] could reasonably be expected to result in immediate and grave harm to [name of applicant]'s [health or safety depending on the circumstances]. However, before releasing the personal information to you, we need to explain to you and obtain your agreement to certain conditions regarding the use and handling of that information that are imposed by section 6 of the Freedom of Information and Protection of Privacy Regulation.

First, you must not use the information except for the purposes of determining whether or not disclosure of the records could reasonably be expected to result in immediate and grave harm to the individual's [specify issue of health or safety].

Second, you accept responsibility for maintaining the security and confidentiality of all personal information found in the records and of any notes you may create from the records.

Third, you agree to [either return all the records and destroy all notes created from the records or destroy all copies of the records and notes taken from them] after you have completed the determination and reported to us.

Once again we thank you for your cooperation. These conditions are established by the Freedom of Information and Protection of Privacy Regulation to protect the privacy of the individual involved and probably reflect confidentiality practices that you already observe in your daily professional activities.



**Model Letter V – Initial letter to expert under section 18(2) (continued)**

Space is provided at the bottom of this letter for you to indicate, through your signature, that you accept these conditions. Please return the letter to us at [name and address of public body]. If you agree to help us in making this determination about disclosure of the information, the records will be forwarded to you shortly.

If you have any questions about the process or section 18(2), do not hesitate to contact me at [telephone number].

Sincerely,

[Name]

[Title]

I agree to the conditions set out above.

---

[Signature of expert]

**Model Letter W – Letter transmitting records to expert under section 18(2)**

*Purpose: To transmit records to an expert for the determination as to whether or not to disclose personal information to an applicant under section 18(2) after they have agreed to the conditions of this process in Model Letter U.*

[Reference number]

[Date]

[Name and address of expert]

Dear [Name of expert]:

[Name of public body] has received your response to our letter of [date of Model Letter V].

Thank you for agreeing to assist us in making a determination whether or not to disclose personal information under section 18(2) of the *Freedom of Information and Protection of Privacy Act*, and for accepting the conditions placed on this assessment.

The records under consideration are enclosed. We would very much appreciate having your opinion by [date].

When you have completed your review, please return the records to [name and address in public body]

OR

When you have completed your review, please [return all the records and destroy all notes created from the records or destroy all copies of the records and notes taken from them] in accordance with the agreement that we have in place with you.

If you have any questions about the process or section 18(2), do not hesitate to contact me at [telephone number].

Sincerely,

[Name]

[Title]

Attachment





## APPENDIX 4

### MODEL FOIP REQUEST CHARTS

**Chart 1: Model FOIP Request (Time limit not extended)**

Key Tasks	Time Lines (Calendar Days)	Manual References	FOIP Tips
Request received by FOIP office. Decision: Routine access to information or FOIP request.	Day of Receipt	2.4 Routine disclosure and active dissemination of information 3.2 Receiving a FOIP request Duty to assist applicant Clarifying requests	Provide information through routine channels if possible.
<b>Thirty-day clock starts</b>	<b>30 calendar days to respond</b>		
Request for access to general records or for the applicant's own personal information? Continuing request? If general access request – initial fee paid? Clarify request with applicant. Decide whether request should be transferred. Send acknowledgement to applicant. Notify applicant if request transferred.	Day 1 - first working day after receipt  <div style="border: 1px solid black; border-radius: 10px; padding: 10px; text-align: center;">Clock does not start until initial fee is paid</div>	1.4 Custody or control 3.2 Receiving a FOIP request Form of the request Acknowledging receipt Continuing requests Clarifying requests Transferring a request	Clarify what is wanted with applicant if not clear. Always be helpful and keep applicant informed. Do not probe motives. Send letter to applicant if initial fee was not received for a general access request. Consult with other public body before transfer.

Key Tasks	Time Lines (Calendar Days)	Manual References	FOIP Tips
<p>Set up request file.</p> <p>Ask program areas to search for records.</p> <p>Log receipt of request on paper or electronic tracking system.</p>	Day 2	<p>3.2 Receiving a FOIP request Documenting and tracking requests</p> <p>3.4 Processing a FOIP request – Search and retrieval Receipt of the request Locating, retrieving and copying records</p>	<p>Information about applicant is only shared on “need to know” basis.</p> <p>Ensure all program areas that may have records are asked to search.</p> <p>Search for all relevant records, including working and electronic files.</p>
<p>Program areas retrieve records and forward originals to FOIP Coordinator.</p> <p>Consider need for time extension if extensive records to be searched.</p> <p>Copy retrieved records.</p>	Days 2 – 7	<p>3.3 Response time limits Time limit extensions</p> <p>3.4 Processing a FOIP request – Search and retrieval Locating, retrieving and copying records</p>	<p>Keep accurate and complete documentation of search.</p> <p>Make three copies of each record and number all documents.</p>
<p>Consider fees and send estimate if applicable with request for deposit.</p> <p>Consider need for consultations within public body and with other public bodies.</p> <p>Consider need for third party consultation.</p> <p>Consider creation of a record.</p> <p>If applicable, send notices to third party – see Chart 2 for process.</p>	<p>Days 7 – 10</p> <div style="border: 1px solid black; border-radius: 10px; padding: 10px; text-align: center;"> <p><b>If fee estimate is sent to applicant, clock stops until deposit is received.</b></p> </div>	<p>3.2 Receiving a FOIP request Consultation</p> <p>3.4 Processing a FOIP request – Search and retrieval Preliminary assessment</p> <p>3.5 Assessing fees</p> <p>3.7 Processing a FOIP request – Reviewing and preparing records for disclosure Creating a new record</p> <p>5 Third Party Notice</p>	<p>Determine whether all relevant records have been located.</p> <p>Stop request processing until deposit is received.</p> <p>Consider fee waiver and/or narrowing request.</p> <p>Executive Council or Treasury Board must be consulted regarding Cabinet confidences.</p>



<b>Key Tasks</b>	<b>Time Lines (Calendar Days)</b>	<b>Manual References</b>	<b>FOIP Tips</b>
Internal consultations. External consultations. Consider whether time extension is needed to complete consultations. Preliminary assessment complete, consultations in process.	<b>End of Day 10</b>	3.2 Receiving a FOIP request Consultation 3.3 Response time limits Time limit extensions	Consult with program areas for context and sensitivity.  Consult externally, i.e. key government departments or local public bodies.
Detailed line-by-line review. Incorporate results of consultations into review (ongoing). Apply exceptions.	<b>Days 10 – 17</b>	3.7 Processing a FOIP request – Reviewing and preparing records for disclosure Line-by-line review of records Severing information 4 Exceptions to the Right of Access	Continue consultation with program areas.  Keep accurate and complete record of reasons for each exception.  Keep accurate records of time spent severing records if fee estimate was issued.
Last day for transferring request.	<b>Day 15</b>	3.2 Receiving a FOIP request Transferring a request	Notify applicant.
FOIP Coordinator reviews recommendations and incorporates results of consultations.  Consider whether time extension is needed to deal with outstanding external consultations.	<b>Day 17 – 21</b>	3.3 Response time limits Time limit extensions 3.7 Processing a FOIP request – Reviewing and preparing records for disclosure	Advise senior management and communications on significant issues.  Encourage public bodies to respond immediately to avoid time extension.
Final consultations, internal and external completed.	<b>End of Day 23</b>		

Key Tasks	Time Lines (Calendar Days)	Manual References	FOIP Tips
Final analysis of review and recommendations. FOIP Coordinator makes final recommendations to decision-maker or makes final decisions.	End of Day 25		Discuss any sensitive or major issue with Head or senior management.
Make any changes required by Head or final decision-maker.  Prepare records for delivery to applicant.	Days 25 – 27	3.7 Processing a FOIP request – Reviewing and preparing records for disclosure  Severing information	
Finalize fee if necessary, and inform applicant in writing of balance owing.	Day 27  <b>Clock stops until balance of fee received</b>	3.5 Assessing fees	
Final response letter to applicant, enclosing records or stating how they may be obtained or examined.  Close file.	Day 30, or next working day if Day 30 falls on weekend or holiday.	3.8 Responding to an applicant  3.9 Completion of request and closure of request file	Ensure all correspondence and documentation is on file.

**Chart 2: Model FOIP Request (Time limit extended for third party notice)**

<b>Key Tasks</b>	<b>Time Lines (Calendar Days)</b>	<b>Manual References</b>	<b>FOIP Tips</b>
Request received by FOIP office. Decision: Routine access to information or FOIP request.	<b>Day of Receipt</b>	2.4 Routine disclosure and active dissemination of information 3.2 Receiving a FOIP request Duty to assist applicant Clarifying requests	Provide information through routine channels if possible.
<b>Thirty Day Clock Starts</b>	<b>30 calendar days to respond</b>		
Request for access to general records or for the applicant's own personal information? Continuing request? If general access request – initial fee paid? Clarify request with applicant. Decide whether request should be transferred. Send acknowledgement to applicant. Notify applicant if request transferred.	<b>Day 1 - first working day after receipt</b>  <div><b>Clock does not start until initial fee is paid</b></div>	1.4 Custody or control 3.2 Receiving a FOIP request Form of the request Acknowledging receipt Continuing requests Clarifying requests Transferring a request	Clarify what is wanted with applicant if not clear. Always be helpful and keep applicant informed. Do not probe motives. Send letter to applicant if initial fee was not received for a general access request. Consult with other public body before transfer.
Set up request file. Ask program areas to search for records. Log receipt of request on paper or electronic tracking system.	<b>Day 2</b>	3.2 Receiving a FOIP request Documenting and tracking requests 3.4 Processing a FOIP request – Search and retrieval Receipt of the request Locating, retrieving and copying records	Information about applicant is only shared on “need to know” basis. Ensure all program areas that may have records are asked to search. Search for all relevant records, including working and electronic files.

Key Tasks	Time Lines (Calendar Days)	Manual References	FOIP Tips
<p>Program areas retrieve records and forward originals to FOIP Coordinator.</p> <p>Copy retrieved records.</p>	<p><b>Days 2 – 7</b></p>	<p>3.3 Response time limits</p> <p>3.4 Processing a FOIP request – Search and retrieval</p> <p>Locating, retrieving and copying records</p>	<p>Keep accurate and complete documentation of search.</p> <p>Make 3 copies of each record and number all documents.</p>
<p>Consider fees and send estimate if applicable with request for deposit.</p> <p>Consider need for consultations within public body and with other public bodies.</p> <p>Consider need for third party consultation.</p> <p>Send notices to third party and applicant.</p> <p>Consider creation of a record.</p>	<p><b>Days 7 – 10</b></p> <div> <p><b>If fee estimate is sent to applicant, clock stops until deposit is received.</b></p> </div>	<p>3.2 Receiving a FOIP request</p> <p>Consultation</p> <p>3.4 Processing a FOIP request – Search and retrieval</p> <p>Preliminary assessment</p> <p>3.5 Assessing fees</p> <p>3.7 Processing a FOIP request – Reviewing and preparing records for disclosure</p> <p>Creating a new record</p> <p>5 Third Party Notice</p>	<p>Determine whether all relevant records have been located.</p> <p>Stop request processing until deposit is received.</p> <p>Consider fee waiver and/or narrowing request.</p> <p>Send third party notices as early as possible.</p> <p>Notify applicant of third party consultations and date by which release decision will be made.</p> <p>Executive Council or Treasury Board must be consulted regarding Cabinet confidences.</p>
<p><b>Decision on release of third party records made after response received from third party or 21 days after notice was given.</b></p>			

Key Tasks	Time Lines (Calendar Days)	Manual References	FOIP Tips
<p>Internal consultations.</p> <p>External consultations.</p> <p>Consider whether time extension is needed to complete consultations.</p> <p>Preliminary assessment complete, consultations in process.</p>	End of Day 10	<p>3.2 Receiving a FOIP request Consultation</p> <p>3.3 Response time limits Time limit extensions</p>	<p>Consult with program areas for context and sensitivity.</p> <p>Consult externally, i.e. key government departments or local public bodies.</p>
<p>Detailed line-by-line review.</p> <p>Incorporate results of consultations into review (ongoing).</p> <p>Apply exceptions.</p>	Days 10 – 17	<p>3.7 Processing a FOIP request – Reviewing and preparing records for disclosure Line-by-line review of records Severing information</p> <p>4 Exceptions to the Right of Access</p>	<p>Continue consultation with program areas.</p> <p>Keep accurate and complete record of reasons for each exception.</p> <p>Keep accurate records of time spent serving records if fee estimate was issued.</p>
Last day for transferring request.	Day 15	<p>3.2 Receiving a FOIP request Transferring a request</p>	Notify applicant.
<p>FOIP Coordinator reviews recommendations and incorporates results of consultations</p> <p>Consider whether time extension is needed to deal with outstanding external consultations.</p>	Day 28-31	<p>3.3 Response time limits Time limit extensions</p> <p>3.7 Processing a FOIP request – Reviewing and preparing records for disclosure</p>	<p>Advise senior management and communications of significant issues.</p> <p>Encourage public bodies to respond immediately to avoid time extension.</p>

Key Tasks	Time Lines (Calendar Days)	Manual References	FOIP Tips
Consider response from third party. Make decision on release of record/severing and send letter to third party and applicant.	Day 32-41	5.6 Response from third party 5.7 Decision by public body and notice of decision	Processing of records not subject to third party notice can continue.
<p><b>Public body has 10 days to make decision regarding disclosure of third party records.</b></p> <p><b>Once the decision is made, third party has 20 days to ask for review.</b></p>			
Final consultations, internal and external completed.	Days 42-57		
Final analysis of review and recommendations. FOIP Coordinator makes final recommendations to decision-maker or makes final decisions.	End of Day 57		Discuss any sensitive or major issue with Head or senior management.
Make any changes required by Head or final decision-maker.  Prepare records for delivery to applicant.	Days 57-59	3.7 Processing a FOIP request – Reviewing and preparing records for disclosure  Severing information	
Finalize fee if necessary, and inform applicant in writing of balance owing.	Day 59  <b>Clock stops until balance of fee received</b>	3.5 Assessing fees	
Final response letter to applicant, enclosing records or stating how they may be obtained or examined.  Close file.	Day 61, or next working day if Day 61 falls on weekend or holiday.	3.8 Responding to applicant 3.9 Completion of request and closure of request file	Ensure all correspondence and documentation is on file.







## **APPENDIX 5**

# **FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY FORMS**

### **Introduction**

These forms are provided in electronic format in the Guidelines and Practices section of the FOIP website ([foip.alberta.ca](http://foip.alberta.ca)) to enable staff of public bodies to download the forms and customize them for their organizations' use.

- Request to Access Information form
- Request Statistics Report
- Transmittal Memorandum (sample)
- Access Request Processing Summary form
- Access Request Recommendation form
- Access Request Recommendation Attachment: Detailed Review of Records form
- Request to Correct Personal Information form
- Annotation to Personal Information form
- Law Enforcement Disclosure form
- Authorization of Representative form (includes Affidavit of Witness form)
- Proposal to Access Personal Information for Research or Statistical Purposes form
- Agreement for Access to Personal Information for Research or Statistical Purposes form
- Office of the Information and Privacy Commissioner - Request for Review form



Request to Access Information

Personal information on this form is collected under Alberta's *Freedom of Information and Protection of Privacy Act* and will be used to respond to your request. See instructions for completing this form.

About you

Title (optional)		Last Name		First Name	
Name of Company or Organization (if applicable)					
Mailing Address		Street	City/Town/Village	Province	Postal Code
Telephone Number (daytime)		Telephone Number (evening)		Fax Number	
( )		( )		( )	
E-mail Address					

About your request

1. What kind of information do you want to access?

☐ General information (An initial fee of \$25 is required – see instructions for explanation of fees.)

☐ Your own personal information (No initial fee is required for personal information.)

2. To which public body are you making your request? (Please fill in the name of the public body that has the records you wish to access. For a complete listing of public bodies, consult the Directory of Public Bodies on the FOIP website at [foip.alberta.ca](http://foip.alberta.ca).)

About the information you want to access

3. Do you want to: ☐ receive a copy of the record? OR ☐ examine the record?

1. What records do you want to access? Please give as much detail as possible. (If you want access to your own personal information, be sure to give all your previous names. For another person's information, you must attach proof that you can legally act for that person.)

2. What is the time period of the records? Please give specific dates. (See instructions for details.)

Your signature

Signature	Date
-----------	------

Where to send your request

Send your completed request form, and initial fee if applicable, to the FOIP Coordinator of the public body that has the records you wish to access. For contact information, consult the Directory of Public Bodies on the FOIP website at [foip.alberta.ca](http://foip.alberta.ca).

FOR OFFICE USE ONLY	
Date Received	Request Number
	Comments

# Request to Access Information

## Instructions

You can access many public body records without making a request under the *Freedom of Information and Protection of Privacy Act* (the *FOIP Act*). To determine whether you need to make a request under the Act or if you need help completing the form, contact the FOIP Coordinator of the public body to which you are making the request.

## About you

In this part of the form enter:

- your last name, first name and preferred title, if any;
- the name of the company or organization you are representing, if applicable;
- your complete mailing address and daytime and evening telephone numbers so that the public body can contact you about the request;
- a fax number or e-mail address, if any, where correspondence may be sent.

## About your request

If you need help to find out what records a public body has, contact the FOIP Coordinator for the public body.

1. **What kind of information do you want to access?**  
Check **general** or **personal** information.

**General information** is information other than personal information (see below). For example, it would include information about a third party.

- There is an initial fee of \$25.00.
  - For a request to a government department, make the cheque payable to the Minister of Finance and Enterprise.
  - For a request to a public body that is **not** a government department, please consult with the FOIP Coordinator for payment information.
- The public body provides you with an estimated cost before processing begins.
- If the total cost of processing your request is more than \$150, you are asked to pay a 50% deposit.
- The records are provided when the fee is paid in full.

**Personal information** is your own personal information or the personal information of an individual you are entitled to represent.

- You must provide proof of your identity before records containing your personal information are released to you.
- If you are requesting records for another person, you must provide proof that you have authority to act for that person (e.g. guardianship or trusteeship order, power of attorney).
- There is no initial fee for accessing your own personal information.
- If the cost of photocopying is more than \$10, you will be notified of the fee.

**Continuing request.** This is a single request that is processed more than once at predetermined time intervals over a period of up to 2 years.

- Contact the FOIP Coordinator of the public body if you are making a continuing request.
- The initial fee is \$50.00.
- You must pay any additional costs as the information becomes available.

2. **To which public body are you making your request?** Enter the name of the public body that you believe has the records that you are requesting.
3. **Do you want to receive a copy of the record OR examine the record?** Check the appropriate box indicating whether you want to receive a copy of the record *or* examine the record.

## About the information you want to access

1. **What records do you want to access?**

- Be as specific as possible in describing the records.
- If you need more space, continue your description on a separate sheet of paper and attach it to this request form.

**If requesting your own personal information, give:**

- your full name;
- any other names that you have previously used; and
- any identifying number that relates to the records, such as your employee number, case number or other identification number.

**If requesting another person's information, give:**

- the person's full name;
- any other name that person may have used on the records; and
- any identifying numbers for the person, if you know them.

**If you are requesting records for another person, you will have to provide proof that you have authority to act for that person.**

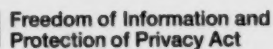
2. **What is the time period of the records?** Enter the specific dates or date ranges of the records you want to access. (e.g. if you want records for the period January 1, 2005 to August 31, 2007, enter those dates. If you want records from August 2008 to present, enter "August 2008 to present.")

## Your signature

Sign and date the form.

## Where to send your request

Send your completed form, and initial fee if applicable, to the FOIP Coordinator of the public body that has the records you wish to access. For contact information, consult the Directory of Public Bodies available on the FOIP website at [foip.alberta.ca](http://foip.alberta.ca).



## Request Statistics Report

[illegible]

**<sup>1</sup> SOURCE OF REQUEST**

- A Academic/Researcher  
B Business/Commercial  
E Elected Official  
M Media  
P General Public  
O Organization/Interest Group

### **3 DISPOSITION CODES**

- |   |                      |
|---|----------------------|
| A | Disclosed completely |
| B | Disclosed partly     |
| C | Nothing disclosed    |
| D | Publicly available   |
| E | Records do not exist |
| F | Abandoned            |
| G | Withdrawn            |
| H | Transferred          |
| I | Disregarded          |

### Correction of Personal Information

- H Correction made  
I Notation placed on record  
J Other disposition

**4 EXTENSION - REASON AND NUMBER OF DAYS REQUIRED**

- EBC - By Commissioner s.14(1)  
ECO - Consultation with other public body s.14(1)(c)  
ECR - Clarify request s.14(1)(a)  
EMC - Multiple concurrent requests s.14(2)  
ESV - Search/volume s.14(1)(b)  
ETN - Third party notice s.14(3)

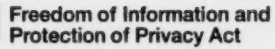
## 5 METHOD OF ACCESS

- C - Copies given  
E - Examination  
B - Both copies and examination  
N/A - Not applicable

**6** Record all exceptions or exclusions cited on the request.

(continued on page 2)





SA 11F (2009/05)

## Transmittal Memorandum (sample)

Date:

To: [Program Director or Records Manager]

From: [FOIP Coordinator]

Re: [subject]

A request under the *Freedom of Information and Protection of Privacy Act* for records relating to [subject] was received on [date]. We have 30 calendar days until [date] in which to respond to it. I would appreciate your immediate attention in locating all relevant records pertinent to the request and a preliminary assessment undertaken in cooperation with my staff by [date]. The FOIP officer assigned to this case is [name and telephone number].

Attached is an Access Request Processing Summary form, an Access Request Recommendation form and a Detailed Review of Records form, which will assist you in documenting the activities and actions connected with the request. This record will be extremely important in developing the [public body's] case if the applicant requests a review by the Information and Privacy Commissioner.

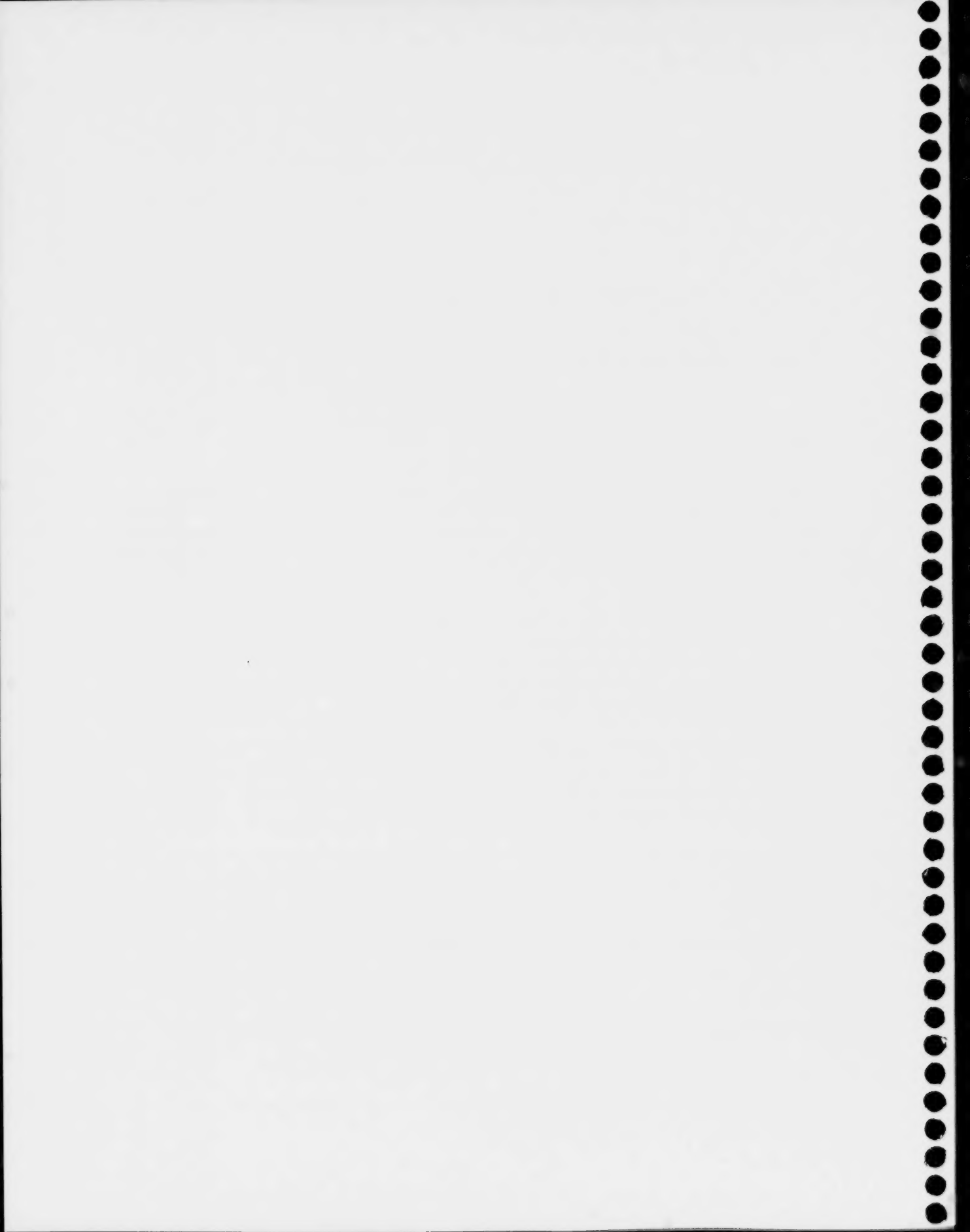
You should be aware that it is an offence under the *Act* to alter, falsify or conceal any record or direct another person to do so (section 92(1)(e)), or to destroy any record (section 92(1)(g)) in order to evade a FOIP request for access to records. The penalty for an offence under section 92 is a fine of up to \$10,000.

Please provide the name(s) of the member(s) of your staff assigned to deal with this request by [date] so that arrangements may be made for a meeting to discuss the [public body's] response.

If you have any questions, please call me at [telephone number].

[FOIP Coordinator]

Attachment





## Access Request Processing Summary

Request Number

Request Type ☐ General Records ☐ Personal Information

Method of Access Requested ☐ Examine Originals ☐ Copies of Records ☐ Copies and Examine Originals

### Tracking Dates

Date Received	Request Due Date	Revised Due Date	Request Close Date
---------------	------------------	------------------	--------------------

### Program Area(s) / Business Unit

Name of Contact(s) and Telephone Number(s)	Name of Contact(s) and Telephone Number(s)
--	--

### Search Completed By

Name (print)	Start Date	Target Completion Date	Actual Completion Date
--------------	------------	------------------------	------------------------

### Preliminary Review Completed By

Name (print)	Start Date	Target Completion Date	Actual Completion Date
--------------	------------	------------------------	------------------------

### Areas Searched (attach file list or other finding aids)

### Records Retrieved - by title

### Staff Time Spent on Locating and Retrieving Records (this time is chargeable)

Name	Total Hours Spent
Name	Total Hours Spent

### Recommendations (e.g. sensitivities, exceptions, potential third parties)

(Attach a separate sheet if more space is required)

Approved by:

Signature of Program Director

Print Name

Date



## Access Request Processing Summary

Request Number

### FOIP Office Review of Records

Records Reviewed By ( <i>print name</i> )	Start Date	Target Completion Date	Actual Completion Date

### FOIP Office Time Spent

Reviewing Records

Name	Total Hours

Severing Records

Name	Total Hours

Preparing Response Package  
(*this time is chargeable*)

Name	Total Hours

### FOIP Office Recommendations

**Prepared by**

**Approved by**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Signature of FOIP Coordinator

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

**foip**Freedom of Information and  
Protection of Privacy Act**Access Request Recommendation**  
**(Decision by Head)**

Request Number

**Request Type** ☐ General Records ☐ Personal Information

To

Date

From

Name of Applicant

Records/Information Requested (*attach detailed review of records if applicable*)

Number of Files/Pages Reviewed

Types of Information Contained in the Records

Exceptions Recommended

Application of Discretionary Exceptions (*summarize reasons*)Application of Mandatory Exceptions (*summarize reasons*)Severing Required (*summarize reasons*)**Prepared by****Approved by**

Signature

Signature of Head

Title

Title

Date

Date





Freedom of Information and  
Protection of Privacy Act

**Access Request  
Recommendation Attachment  
Detailed Review of Records**

Request Number	Name of Public Body		Program Area	Business Unit		Program Area Contact	Telephone Number
Record Number	Number of Pages	Record Date	Record Description	Exceptions Applied	Exclusions	Comments/Explanations	Third Party Notice or Consultation (Yes or No)



## Request to Correct Personal Information

Personal information on this form is collected under Alberta's *Freedom of Information and Protection of Privacy Act* and will be used to respond to your request. See instructions for completing this form.

### About you

Title (optional)	Last Name	First Name		
Mailing Address	Street	City/Town/Village	Province	Postal Code
Telephone Number (daytime) ( )	Telephone Number (evening) ( )		Fax Number ( )	
E-mail Address				

### About your request

**1. Whose information do you want to correct?**

- ☐ Your own personal information
- ☐ Another person's information (Please attach proof that you can legally act for the person.)

**2. To which public body are you making your request?** (Please fill in the name of the public body that has the records you want corrected. For a complete listing of public bodies, consult the Directory of Public Bodies on the FOIP website at [foip.alberta.ca](http://foip.alberta.ca).)

--

### About the information you want to correct

**1. What personal information needs to be corrected?** (Please give as much detail as possible. Be sure to give the complete name that is in the records if it is different from the name given above.)

--

**2. What correction do you want to make and why?** (Please attach any documents that support your request.)

--

### Your signature

Signature	Date
-----------	------

### Where to send your request

Send your completed request form to the FOIP Coordinator of the public body that has the records you want corrected. For contact information, consult the Directory of Public Bodies on the FOIP website at [foip.alberta.ca](http://foip.alberta.ca).

FOR OFFICE USE ONLY	
Date Received	Request Number
	Comments

# Request to Correct Personal Information

## Instructions

You can correct information in many public body records without making a request under the *Freedom of Information and Protection of Privacy Act* (the *FOIP Act*). To determine whether you need to make a request under the Act or if you need help completing the form, contact the FOIP Coordinator of the public body to which you are making the request.

## About you

In this part of the form enter:

- your last name, first name and preferred title, if any;
- your complete mailing address and daytime and evening telephone numbers so that public body can contact you about the request; and
- a fax number or e-mail address, if any, where correspondence may be sent.

## About your request

1. Whose information do you want to correct? Indicate whether you want your personal information or another person's information to be corrected.

### Your personal information

If you want your information to be corrected, you will have to provide proof of your identity.

### Another person's information

If you want the information of another person to be corrected, you will have to provide proof that you have the authority to act for that person. For example, you might provide proof that you are the person's guardian or trustee or that you have power of attorney for the person.

2. Enter the name of the public body that you believe has the records that you want corrected.

## About the information you want to correct

1. What records contain the information that you want corrected?
  - Be as specific as possible in describing the records. The more specific your request, the more quickly and accurately it can be answered.
  - If you need more space, please continue your description on a separate sheet of paper and attach it to this form.

If you want a correction made to your own personal information, please be sure that you give:

- your full name;
- any other names that you have used on the records; and
- any identifying number that relates to the records, such as your employee number, case number or other identification number.

If you want a correction made to another person's information, please give:

- the person's full name;
- any other name that person may have used on the records; and
- any identifying numbers for the person if you know them.

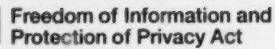
2. What correction do you want made? What is incorrect about the information that is currently on the record? Please be specific.

## Your signature

Sign and date the form.

## Where to send your request

Send your completed form to the FOIP Coordinator of the public body that has the records you want corrected. For contact information, consult the Directory of Public Bodies available on the FOIP website at [foip.alberta.ca](http://foip.alberta.ca)



Name of Personal Information Bank	Number of Personal Information Bank	Reference Number
-----------------------------------	-------------------------------------	------------------

Name of Public Body

---

Print Name

Signature

Date





Freedom of Information and  
Protection of Privacy Act

## Law Enforcement Disclosure

Request for Disclosure under Section 40(1)(q) of the  
Freedom of Information and Protection of Privacy Act

Date

In accordance with section 40(1)(q) of the *Freedom of Information and Protection of Privacy Act*, the

Name of Public Body

requests disclosure of personal information pertaining to

Name of Individual or Other Identifier

which may be generally described as:

General Description of Information Requested

This information is required by this public body to assist in an investigation pursuant to:

Reference to a Federal or Provincial Statute or Local Public Body Bylaw by Section or Description of Purpose

### Requesting Official

Name

Title

Signature

Badge Number (if applicable)

I, \_\_\_\_\_ ☐ consent to, or ☐ refuse this disclosure  
Name of Disclosing Official  
of personal information.

If disclosure has been authorized, the personal information bank(s) is:

Name(s) of Personal Information Bank(s)

### Authorized Disclosing Official

Name

Title

Signature

Name of Public Body

**NOTE:** This completed record may qualify for exception to disclosure under  
section 20 of the *Freedom of Information and Protection of Privacy Act*.







## Authorization of Representative

I, \_\_\_\_\_,

living at \_\_\_\_\_, in the province of \_\_\_\_\_,

authorize \_\_\_\_\_

living at \_\_\_\_\_, in the province of \_\_\_\_\_,

as my personal representative to act on my behalf, and to exercise:  
(select one)

- ☐ all my rights under the *Freedom of Information and Protection of Privacy Act*
- ☐ my right to access all my records containing personal information in all categories of personal information
- ☐ my right to access all of the following records containing personal information or all of the following categories of personal information (*number and titles of records or categories*):
- ☐ the rights that I have under the *Freedom of Information and Protection of Privacy Act* regarding the following other matters (*e.g. consent to disclose personal information*):

I confirm that my representative has the authority to exercise the above right(s) under the Act for me.

This authorization will be in effect until

Signed By \_\_\_\_\_ in the presence of \_\_\_\_\_  
Signature of Authorizing Person Signature of Witness

(See Affidavit of Witness form to complete)

## Affidavit of Witness

CANADA

IN THE PROVINCE OF ALBERTA

I, \_\_\_\_\_  
Name of the Witness in Full

\_\_\_\_\_  
Occupation of Witness

of \_\_\_\_\_  
Complete Home Address of Witness

in the province of \_\_\_\_\_, make oath and say that:

1. I was personally present and I saw \_\_\_\_\_  
Name of Individual  
sign the Authorization of Representative form to which this is attached.

2. The Authorization of Representative form was signed by \_\_\_\_\_  
Name of Individual  
at \_\_\_\_\_, in the province of \_\_\_\_\_  
and that I am the one who witnessed the form.

3. I know \_\_\_\_\_ and I believe that he/she is  
Name of Individual  
18 years of age or older.

\_\_\_\_\_  
Signature of Witness

Sworn before me at \_\_\_\_\_ )  
in the province of \_\_\_\_\_ )  
on \_\_\_\_\_ )

\_\_\_\_\_  
Commissioner for Oaths

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Expiry Date of Commission

**foip**Freedom of Information and  
Protection of Privacy Act

---

Name of Public Body

**Proposal  
to  
Access Personal Information  
for  
Research or Statistical Purposes**

This form is used to request access, for research or statistical purposes, to personal information contained in records covered by the *Freedom of Information and Protection of Privacy Act* (the *FOIP Act*). If this request is approved by \_\_\_\_\_,

Name of Public Body

you will be asked, prior to being provided access to records containing personal information, to sign a research agreement that ensures that individuals' privacy will be protected when their personal information is in your custody.

The collection of the information on this form is authorized by the *Act* and will be used only to evaluate and administer the request for access to personal information for the purpose of research.

The following person can answer any questions concerning this proposal or the collection of the information on this form.

Name of Contact: \_\_\_\_\_

Title: \_\_\_\_\_

Name of Public Body: \_\_\_\_\_

Business Address: \_\_\_\_\_

Business Telephone Number: (     ) \_\_\_\_\_

Completeness and clarity will assist the

---

Name of Public Body

to assess this proposal quickly.

**NOTE: A fee may be charged to provide this information. An estimate of the fee will be provided in advance.**

## Proposal to Access Personal Information for Research or Statistical Purposes

### Identification of Researcher

Name (Last, First, Initials)				
Mailing Address	Street	City/Town/Village	Province	Postal Code
Telephone Number (      )		Fax Number (      )		
E-mail Address				

### Provide the following additional information, if applicable:

Institutional, Society or Corporate Affiliation (include department if relevant)
Position
Provide the name of your Academic Advisor if you are a student

**Provide a curriculum vitae including the following information: education, research experience, and knowledge of subject.**

### Description of Research Project

Attach the following information:

1. A general description of the research project (*include the objectives of the project and the proposed method(s) of analysis*).
2. An explanation of why the research project cannot be accomplished without access to personal information about named or identifiable individuals.
3. A detailed explanation of how the personal information will be used, including a description of any proposed linkages to be made between personal information in the records requested and any other personal information.
4. The expected period of time during which access to these records may be required.
5. The expected period of time during which these records will be used.
6. The benefits to be derived from the research project.
7. Describe the security measures you propose to put in place. The security and confidentiality of the personal information that will be in your custody must be protected and unauthorized disclosure must not occur.

**Proposal to Access Personal Information  
for Research or Statistical Purposes**

**Funding**

Has funding to complete the project already been approved or received? ☐ Yes ☐ No

If funding is not already in place, explain the conditions and circumstances that will allow the project to be completed.

**Additional Information**

Please add any other information that you believe will assist

\_\_\_\_\_ in assessing this application.

Name of Public Body



**Proposal to Access Personal Information  
for Research or Statistical Purposes**

**Records Requested**

Describe all records containing personal information to which access is requested. Provide as much detail as possible. Access will be given only to records listed below and only for the purposes approved for the research project described on Page 2 of this form. Any changes or additions to this list after the application is submitted should be made in writing and will require approval in writing from

---

Name of Public Body

**Proposal to Access Personal Information  
for Research or Statistical Purposes**

**Records Requested - Continued**

Originals may be viewed only at

\_\_\_\_\_  
Name of Public Body

Will you require the above records to be copied (at your expense) for viewing elsewhere? ☐ Yes ☐ No

**FOR PUBLIC BODY USE ONLY**

The application for records pursuant to Section 42 or Section 43 of the Act is approved subject to the terms and conditions of a corresponding research agreement.

\_\_\_\_\_  
Signature of Authorized Official

\_\_\_\_\_  
Position

\_\_\_\_\_  
Date





Freedom of Information and  
Protection of Privacy Act

---

Name of Public Body

**Agreement  
for  
Access to Personal Information  
for  
Research or Statistical Purposes**

This agreement is used only when a Proposal to Access Personal Information for Research or Statistical Purposes ("the Proposal") has been approved. The Proposal must be appended to this agreement and forms part of the agreement.

**BETWEEN:**

---

Name of Researcher

**AND:**

---

Name of Public Body

**Description of Research Project**

The research project for which the accessed records will be used is referred to in this agreement as:

Details of the purpose of the research, how the information will be used, and linkages that will be done are included in the Proposal.

**Agreement for Access to Personal Information  
for Research or Statistical Purposes**

**Records Requested**

Only those records requested in the Proposal will be provided ("the records"). Any changes or additions to the list must be made in writing and will require approval in writing from

---

Name of Public Body

Clarification of the records requested is shown below if required.

In the event that there is a difference between the records requested above and the records requested in the Proposal, the information about records requested in this agreement governs the agreement.

The expiry date for access to the records listed in the Proposal and this Agreement is \_\_\_\_\_  
(year/month/day)

## Agreement for Access to Personal Information for Research or Statistical Purposes

### Fee

The Researcher is responsible for paying any fees incurred by

\_\_\_\_\_  
Name of Public Body

to search for, copy and or provide the records.

The estimated fee is \$ \_\_\_\_\_.

The Researcher understands that this estimate may be revised at any time by

\_\_\_\_\_  
Name of Public Body

and any revision will be made in writing.

### Approval of Terms and Conditions of Access

\_\_\_\_\_  
Name of Public Body

approves the following terms and conditions of access.

\_\_\_\_\_  
Name of Public Body

reserves the right to withdraw access to the records without prior written notice if this becomes necessary under the Act.

### Terms and Conditions of Access

The Researcher understands and will abide by the following terms and conditions:

#### Security

1. The Researcher is responsible for maintaining the security and confidentiality of all personal information found in or taken from the records.
2. The Researcher, and only the following persons, will have access to this personal information in a form that identifies, or could be used to identify, the individual(s) to whom it relates:

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Before any personal information is disclosed to the persons listed above, the Researcher will obtain a written agreement from each of them to ensure they will not disclose that personal information to any other person and will be bound by all terms and conditions of the present agreement. The Researcher will keep a copy of each such agreement, and will provide

\_\_\_\_\_  
Name of Public Body

with a photocopy of each agreement.



**Agreement for Access to Personal Information  
for Research or Statistical Purposes**

3. None of the records (including copies of them or notes containing personal information taken from them) will be left unattended at any time, except under the conditions described in Clauses 4, 5 and 6, below. If the Researcher is using the records on the premises of

\_\_\_\_\_  
Name of Public Body

the Researcher will comply with the security procedures of

\_\_\_\_\_  
Name of Public Body

4. Any copies of the records and any notes which contain personal information taken from them will be kept at the following address(es):

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

No records will be removed from the above premises without the prior written consent of

\_\_\_\_\_  
Name of Public Body

5. Physical security at the above premises will be maintained by ensuring that the premises are securely locked, except when one or more of the individuals named in Clause 2 are present, as well as by the following additional measures (e.g. locked filing cabinet):

## Agreement for Access to Personal Information for Research or Statistical Purposes

### Security Continued

6. Individually identifiable information from the records will be maintained on a computer system to which users, other than those listed in Clause 2, have access.

☐ Yes ☐ No

If yes, access to the information will be restricted through the use of passwords and by other computer security measures that prevent unauthorized access, and can trace such unauthorized access, including the following methods:

7.

\_\_\_\_\_  
Name of Public Body

will be permitted to carry out on-site visits and such other inspections or investigations that it deems necessary to ensure compliance with the conditions of this agreement.

### Use of Personal Information

8. Personal information contained in the records will not be used or disclosed for any purpose other than the research project described in the proposal (including additional linkages between sources of personal information), nor for any subsequent purpose, without the express written permission of

\_\_\_\_\_  
Name of Public Body

9. Papers or any other works which describe the results of the research undertaken will be written and/or presented in such a way that no individuals referred to in the records can be identified and no linkages can be made between any personal information found in the records and personal information that is publicly available from other sources. There will be no exceptions to this rule without prior and specific written permission from

\_\_\_\_\_  
Name of Public Body

10. Any case file numbers or other individual identifiers to be recorded on computer will be created by the Researcher or one of the persons listed in Clause 2 and will not relate to any real case numbers found in the records. Any such identifiers are to be used for statistical purposes only.
11. No case file numbers or other individual identifiers assigned for the purposes of the research project will appear in any other work.

## Agreement for Access to Personal Information for Research or Statistical Purposes

### Use of Personal Information Continued

12. No personal information that identifies or could be used to identify the individual(s) to whom it relates will be transmitted by means of any telecommunications device, including telephone, fax, cable, and wireless communication networks.

13. Unless expressly authorized in writing by

---

Name of Public Body

no direct or indirect contact will be made with the individuals to whom the personal information relates.

14. Individual identifiers associated with the records, or contained in copies of them, will be removed or destroyed at the earliest time at which removal or destruction can be accomplished consistent with the research purpose. At the latest, this will occur by: \_\_\_\_\_  
(year/month/day)

Any extension to this time limit must be approved in writing by

---

Name of Public Body

The removal of individual identifiers will be done in a manner that ensures that remaining personal information (including any found in research notes) cannot be used to identify the individual to whom it relates. **If necessary, this will be done by destroying copies of records or pages of notes in their entirety.** All destruction or removal of individual identifiers will be confidential and complete in order to prevent access by any unauthorized persons.

15. The Researcher is responsible for ensuring complete compliance with these terms and conditions. In the event that the Researcher becomes aware of a breach of any of the conditions of this agreement, the Researcher will immediately notify

---

Name of Public Body

in writing.

16. The Researcher understands that the *Freedom of Information and Protection of Privacy Act* specifies that a person who under the Act wilfully contravenes the Act's requirements for collection, use and disclosure of personal information is guilty of an offence and liable to a fine of up to \$10,000. In addition to liability for an offence, the Researcher understands that

---

Name of Public Body

may take legal action against the Researcher if there is contravention of the terms and conditions of this agreement.

17. Written consent of

---

Name of Public Body

must be obtained prior to the transfer of this agreement to another person, or a change in the use of the information is implemented. Consent may be arbitrarily withheld at the sole discretion of

---

Name of Public Body

**Agreement for Access to Personal Information  
for Research or Statistical Purposes**

**Use of Personal Information Continued**

18. \_\_\_\_\_  
Name of Public Body

will receive a copy of the final research product.

Signed at \_\_\_\_\_, on \_\_\_\_\_  
City/Town/Village Date

\_\_\_\_\_  
Signature of Researcher

\_\_\_\_\_  
Signature of Witness

\_\_\_\_\_  
Name and Position of Witness

\_\_\_\_\_  
Signature of Authorized Official of Public Body

\_\_\_\_\_  
Date

\_\_\_\_\_  
Position





Office of the Information  
And Privacy Commissioner

## REQUEST FOR REVIEW

### *Freedom of Information and Protection of Privacy Act*

**TO: Information and Privacy Commissioner of Alberta**  
Suite 410, 9925 – 109 Street  
Edmonton, Alberta T5K 2J8  
Phone: (780) 422-6860 or 1-888-878-4044  
Fax: (780) 422-5682

Applicant's Name:

Applicant's Mailing Address:

Applicant's Daytime Phone Number

Under the *Freedom of Information and Protection of Privacy Act* “(the FOIP Act)”, the Commissioner is authorized to review the decisions of public bodies to ensure compliance with the FOIP Act.

**I am requesting a review by the Commissioner for 1 or more of the following reasons:**

☐ I applied for access to information under the FOIP Act from: \_\_\_\_\_  
(name of Public Body)  
(Please attach a copy of your access request to the public body and a copy of the Public Body's letter responding to your request)

☐ I asked to have my information corrected by: \_\_\_\_\_  
(name of Public Body)  
(Please attach a copy of your request to the public body for correction and a copy of the Public Body's letter responding to your request)

☐ I have been notified that information about me or my business will be released by: \_\_\_\_\_  
(name of Public Body)  
in response to an access application (please attach a copy of the Public Body's notification letter).  
*Note: This request must be received by the Commissioner's office within 20 days after you have notified by the public body of this decision.*

**Please provide an explanation as to what you want reviewed:** *(attach additional pages as required)*

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

**Note:** Under the FOIP Act, the Commissioner's Office is required to provide a copy of your completed form to the head of the public body concerned and to any other person who in the opinion of the Commissioner is affected by the request. If you have concerns with this requirement, please make them known to the Commissioner's Office immediately.









# **FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT AND REGULATION CITATIONS INDEX**



## Freedom of Information and Protection of Privacy Act and Regulation Citations

### ***Freedom of Information and Protection of Privacy Act***

Part 1	13, 18-19, 31, 51, 98, 115, 233, 264, 265, 267, 317, 350, 355
section 1	2-5, 6-7
section 1(b.1)	7
section 1(d)	2-3
section 1(e)	115, 141, 275
section 1(f)(i)	23
section 1(f)(ii)	23
section 1(f)(iii)	23
section 1(f)(iv)	23
section 1(g)	3
section 1(h)	124, 145, 174, 237, 243, 282, 283
section 1(i)	3-4, 4
section 1(j)	2, 153
section 1(m)	288
section 1(n)	6-7, 18, 56, 113, 233, 254, 337
section 1(n)(vi)	55
section 1(p)	2, 4, 283
section 1(q)	6, 55
section 1(r)	102, 211, 214
section 1(s)	102, 190
section 2	1
section 2(e)	349
section 3(a)	5, 31, 58, 207
section 3(b)	5, 300
section 3(c)	5
section 3(d)	6
section 3(e)	6, 94, 259, 282, 300
section 3(e)(ii)	253, 306
section 4	2, 18, 71, 85, 91, 95
section 4(1)	6, 353
section 4(1)(a)	9
section 4(1)(b)	9-10
section 4(1)(c)	10
section 4(1)(d)	10-11, 19
section 4(1)(e)	11
section 4(1)(f)	11
section 4(1)(g)	11
section 4(1)(h)	11
section 4(1)(i)	11-12
section 4(1)(j)	12, 300

section 4(1)(j.1)	6, 12
section 4(1)(k)	12-13
section 4(1)(l)	13-14
section 4(1)(l)(ii)	14
section 4(1)(l)(vi)	14
section 4(1)(m)	14-15, 16
section 4(1)(n)	15-16
section 4(1)(o)	15
section 4(1)(p)	16
section 4(1)(q)	16-17, 166
section 4(1)(r)	17, 18
section 4(1)(s)	17-18
section 4(1)(t)	18
section 4(1)(u)	18, 55, 56, 288
section 4(2)	15, 173
section 4(3)	9
section 4(4)	17, 111
section 5	20-21, 25, 95, 97, 269, 302
section 6	18-19
section 6(1)	47, 95
section 6(2)	82, 85, 204
section 6(3)	49, 77
section 6(4)	18-19
section 6(4)(a)	18
section 6(4)(b)	19
section 6(5)	18-19
section 6(6)	19
section 6(7)	19, 177
section 6(8)	186
section 6(8)(a)	19
section 6(8)(b)	19
section 7	50, 51, 52
section 7(1)	49, 53
section 7(2)	49, 53
section 7(3)	49, 90
section 8	81
section 9	212
section 10	350, 356, 362
section 10(1)	32, 50, 51, 52, 60, 68, 89
section 10(2)	73, 83
section 11	49
section 11(1)	64, 215
section 11(2)	64



section 11(4).....	73	section 17(2)(c).....	115, 131
section 12(1).....	87, 88, 92, 93, 135, 139, 208	section 17(2)(e).....	115, 116, 117, 118, 120, 126, 267
section 12(1)(c).....	90, 159	section 17(2)(f).....	115, 118, 268
section 12(1)(c)(i).....	87	section 17(2)(g).....	117, 118, 119, 268
section 12(2).....	88, 92, 135, 158	section 17(2)(h).....	117, 119, 120, 268
section 12(2)(a).....	139, 158	section 17(2)(i).....	100, 120, 268, 301
section 12(2)(b).....	135, 159	section 17(2)(j).....	120, 121, 123, 126, 213, 268,
section 13(2).....	90	section 17(2)(j)(i).....	121
section 13(2)(b).....	90	section 17(2)(j)(iii).....	122
section 14.....	63, 64, 215, 258, 350, 356, 362	section 17(2)(j)(iv).....	122
section 14(1).....	66, 67, 215, 216	section 17(3).....	120, 121, 123, 213
section 14(1)(a).....	54, 65, 215, 258	section 17(4).....	123, 124, 125, 129
section 14(1)(b).....	65, 215, 258	section 17(4)(a).....	124
section 14(1)(c).....	65, 215	section 17(4)(b).....	124, 125, 151
section 14(1)(d).....	65	section 17(4)(c).....	125
section 14(2).....	66, 67, 215	section 17(4)(d).....	126, 213
section 14(3).....	65, 215, 216	section 17(4)(e).....	127
section 14(4).....	67	section 17(4)(e.1).....	127
section 15.....	20, 64	section 17(4)(f).....	117, 127
section 15(1).....	62	section 17(4)(g).....	128
section 15(2).....	63	section 17(4)(g)(i).....	128
section 15.1.....	56	section 17(4)(g)(ii).....	128
section 16.....	17, 40, 99, 100, 103, 111, 118, 191, 211, 212, 213, 214, 218, 219, 232, 267, 302, 337, 355, 361	section 17(4)(h).....	128
section 16(1).....	96, 101, 103, 110	section 17(5).....	116, 123, 129, 151, 291
section 16(1)(a).....	101, 190	section 17(5)(a).....	130
section 16(1)(b).....	101, 104, 133	section 17(5)(b).....	130, 131
section 16(1)(c).....	101, 106, 191, 212	section 17(5)(c).....	131, 132
section 16(1)(c)(i).....	106	section 17(5)(d).....	132
section 16(1)(c)(ii).....	106-107	section 17(5)(e).....	132
section 16(1)(c)(iii).....	108	section 17(5)(f).....	132
section 16(1)(c)(iv).....	108, 109	section 17(5)(g).....	134
section 16(2).....	96, 109, 110	section 17(5)(h).....	134
section 16(3).....	110	section 17(5)(i).....	134
section 16(3)(a).....	110	section 18.....	87, 97, 99, 137, 139, 218, 267, 337
section 16(3)(b).....	111	section 18(1).....	137
section 16(3)(c).....	111, 182	section 18(1)(a).....	137
section 16(3)(d).....	111	section 18(1)(b).....	137
section 17.....	20, 40, 92, 96, 113, 114, 135, 211, 212, 213, 214, 218, 219, 225, 232, 233, 267, 291, 301, 337, 355, 361	section 18(2).....	138, 285
section 17(1).....	113, 129	section 18(3).....	139
section 17(2).....	113, 114, 268	section 19.....	97, 141, 143, 267, 337
section 17(2)(a).....	114	section 19(1).....	141, 142, 143
section 17(2)(b).....	39, 115, 131	section 19(2).....	142, 143
		section 19(3).....	142
		section 20.....	92, 99, 100, 145, 158, 159, 218, 267, 284, 302, 337
		section 20(1).....	97, 147, 148, 157

section 20(1)(a).....	148, 152, 156	section 24(1)(a).....	177, 178, 179, 180
section 20(1)(b).....	148,	section 24(1)(b).....	177, 180
section 20(1)(b.1).....	149	section 24(1)(c).....	177, 181
section 20(1)(c).....	150	section 24(1)(d).....	177, 181
section 20(1)(d).....	150, 151	section 24(1)(e).....	172, 177, 182
section 20(1)(e).....	151	section 24(1)(f).....	177, 182
section 20(1)(f).....	152	section 24(1)(g).....	177, 182
section 20(1)(g).....	152, 153	section 24(1)(h).....	177, 183
section 20(1)(h).....	153	section 24(2).....	183
section 20(1)(i).....	153	section 24(2)(a).....	182, 183
section 20(1)(j).....	154	section 24(2)(b).....	184
section 20(1)(k).....	154	section 24(2)(c).....	184
section 20(1)(l).....	154	section 24(2)(d).....	185
section 20(1)(m).....	155	section 24(2)(e).....	185
section 20(1)(n).....	155	section 24(2)(f).....	185, 186
section 20(2).....	153	section 24(2)(g).....	186
section 20(3).....	156, 157	section 24(2.1).....	19, 101, 177, 186
section 20(3)(a).....	156	section 24(2.1)(a).....	96, 186
section 20(3)(b).....	156	section 24(2.1)(b).....	96, 186
section 20(4).....	96, 157	section 24(2.2).....	186
section 20(5).....	157	section 24(2.2)(a).....	186
section 20(5)(a).....	157	section 24(2.2)(b).....	186
section 20(6).....	158	section 24(3).....	183
section 20(6)(a).....	158	section 25.....	97, 99, 188, 189, 193, 218, 267, 337
section 20(6)(b).....	158	section 25(1).....	188, 189, 193
section 21.....	65, 97, 101, 161, 164, 218, 267, 337	section 25(1)(a).....	188, 190
section 21(1).....	161	section 25(1)(b).....	188, 190
section 21(1)(a).....	161, 162, 163	section 25(1)(c).....	188, 191, 192
section 21(1)(b).....	161, 163	section 25(1)(d).....	188, 193
section 21(2).....	163	section 25(2).....	193
section 21(3).....	164	section 25(2)(a).....	103
section 21(4).....	101, 164	section 25(2)(b).....	193
section 22.....	96, 101, 166, 167, 170, 267, 337	section 26.....	97, 195, 267, 337
section 22(1).....	166, 167, 168, 169, 170	section 26(a).....	195
section 22(2).....	168	section 26(b).....	195
section 22(2)(a).....	168	section 26(c).....	195
section 22(2)(b).....	169	section 27.....	97, 196, 197, 204, 218, 267, 302, 337
section 22(2)(c).....	169, 170	section 27(1).....	196, 204
section 23.....	97, 101, 172, 175, 267, 337	section 27(1)(a).....	197, 201, 202, 204
section 23(1).....	172	section 27(1)(b).....	201, 202
section 23(1)(a).....	172, 175	section 27(1)(c).....	202
section 23(1)(b).....	173, 174, 175	section 27(2).....	97, 151, 196, 202, 203, 204, 214, 218
section 23(2)(a).....	175	section 27(3).....	196, 199
section 23(2)(b).....	175	section 28.....	97, 206, 267, 337
section 24.....	166, 177, 186, 214, 218, 267, 337	section 28(a).....	206
section 24(1).....	97, 101, 177, 183, 184, 185, 186		

section 28(b) .....	206	section 34(1)(d).....	234, 242, 320, 321,
section 29 .....	2119-19, 97, 207, 209, 213, 267	section 34(1)(e).....	234, 242, 320, 321,
section 29(1)(a).....	207	section 34(1)(f) .....	234, 243, 320, 321,
section 29(1)(a.1) .....	207	section 34(1)(g).....	234, 237, 243, 245, 320, 321,
section 29(1)(b).....	207, 208, 209	section 34(1)(h).....	234, 244, 320, 321
section 29(2) .....	208	section 34(1)(i).....	234, 244, 320, 321
section 29(3) .....	209	section 34(1)(j).....	234, 245, 320, 321
section 30 .....	39, 40, 65, 66, 67, 93, 211, 212, 213, 214, 215, 216, 218, 219	section 34(1)(k).....	234, 320, 321
section 30(1.1) .....	208	section 34(1)(k)(i).....	245
section 30(1) .....	212, 213, 214, 213	section 34(1)(k)(ii).....	245
section 30(1)(a).....	211	section 34(1)(l).....	234, 246, 320, 321
section 30(1)(b).....	211	section 34(1)(m).....	234, 246, 320, 321
section 30(2) .....	123, 213	section 34(1)(n).....	234, 247, 320, 321
section 30(3) .....		section 34(1)(o).....	234, 248, 320, 321
section 30(4) .....	218	section 34(2) .....	248, 262, 321, 333, 345
section 30(4)(c).....	216	section 34(3) .....	250, 321, 345
section 30(5) .....	215, 219	section 35 .....	250, 251, 320, 345
section 31 .....	39, 40, 66, 93, 215, 216, 222	section 35(a).....	250, 289, 222
section 31(1) .....	216, 219, 221	section 35(b) .....	6, 94, 250, 252, 323, 351
section 31(2) .....	221	section 36 .....	254, 257, 320, 322
section 31(3) .....	216	section 36(1) .....	50, 59, 253, 254, 350, 356, 362
section 31(4) .....	216	section 36(2) .....	254
		section 36(3) .....	256
Part 2 .....	5, 7, 13, 25, 28, 43, 45, 113, 121, 208, 214, 233, 234, 235, 241, 319, 320, 327, 334, 339, 342, 344, 345, 347, 350, 351, 352, 353, 356, 358, 363, 364	section 36(4) .....	257, 266
section 32 .....	43, 96, 98, 109, 115, 204, 225, 226, 227, 228, 229, 230, 232, 265, 267, 351, 353	section 36(5) .....	258
section 32(1) .....	225, 228, 230	section 36(6) .....	258
section 32(1)(a).....	225, 228	section 36(7) .....	258
section 32(1)(b).....	79, 121, 225, 228	section 37 .....	61, 63, 259, 320
section 32(3) .....	230, 231	section 37(2) .....	63
section 32(4) .....	39, 231	section 38 .....	40, 259, 320, 324, 335
section 33 .....	235, 236, 239, 242, 260, 262, 268, 289, 320, 327, 333, 345, 351	Part 2, Division 2 .....	241
section 33(a).....	236, 320	section 39 .....	260, 263, 320, 325, 327, 345
section 33(b) .....	237, 320	section 39(1)(a).....	260, 261, 294
section 33(c).....	237, 238, 248, 320	section 39(1)(b).....	260, 261
section 34 .....	241, 320, 327, 333, 333	section 39(1)(c).....	260, 263
section 34(1) .....	240, 289, 320, 345	section 39(2) .....	260, 263, 293
section 34(1)(a).....	240, 321,	section 39(3) .....	263
section 34(1)(a)(i) .....	241	section 39(4) .....	264
section 34(1)(b).....	234, 241, 320, 321,	section 40 .....	32, 51, 225, 241, 260, 263, 264, 264, 266, 267, 268, 320, 325, 326, 345, 347, 351
section 34(1)(c).....	234, 242, 320, 321,	section 40(1) .....	265, 288, 292, 326
		section 40(1)(a).....	267
		section 40(1)(aa) .....	288, 292
		section 40(1)(bb).....	289
		section 40(1)(bb.1).....	290
		section 40(1)(cc) .....	284, 290, 291, 356

section 40(1)(dd).....	292	section 43(1)(a)(i)(A).....	301
section 40(1)(ee).....	292	section 43(1)(b).....	300, 301, 302
section 40(1)(ff).....	293	section 43(1)(b)(i).....	111
section 40(1)(b).....	121, 214, 266, 267, 301	section 45.....	349
section 40(1)(c).....	268, 294	section 45(3).....	349
section 40(1)(d).....	269, 345	section 47.....	349
section 40(1)(e).....	270, 271, 272, 282, 284	section 51(2).....	364
section 40(1)(f).....	272, 273, 285, 286, 301	section 53.....	45, 349, 363
section 40(1)(g).....	273, 274	section 53(1).....	231, 350, 362, 363
section 40(1)(h).....	274, 275, 276	section 53(1)(a).....	306, 349, 353
section 40(1)(i).....	276, 294	section 53(1)(b).....	350
section 40(1)(j).....	277	section 53(1)(c).....	350
section 40(1)(k).....	277, 278	section 53(1)(d).....	350
section 40(1)(k)(ii).....	278	section 53(1)(e).....	350
section 40(1)(l).....	263, 279	section 53(1)(f).....	329, 350
section 40(1)(m).....	279	section 53(1)(g).....	343, 350
section 40(1)(n).....	280, 281	section 53(1)(h).....	241, 350
section 40(1)(o).....	281	section 53(1)(i).....	350
section 40(1)(p).....	282, 317	section 53(1)(j).....	350, 352
section 40(1)(q).....	282, 283	section 53(2).....	76, 356, 362
section 40(1)(q)(ii).....	283	section 53(2)(a).....	350
section 40(1)(r).....	284	section 53(2)(b).....	350
section 40(1)(r)(ii).....	284	section 53(2)(c).....	350
section 40(1)(s).....	284	section 53(2)(d).....	350
section 40(1)(t).....	284	section 53(2)(e).....	350, 363
section 40(1)(u).....	285	section 54.....	353
section 40(1)(v).....	285	section 54(1).....	352
section 40(1)(w).....	286	section 54(2).....	352
section 40(1)(x).....	286, 287	section 55.....	56, 354
section 40(1)(y).....	287	section 55(1).....	57, 58, 59
section 40(1)(z).....	288	section 55(1)(a).....	57
section 40(2).....	265, 293, 294	section 55(1)(b).....	57, 59
section 40(3).....	265, 292, 294, 326	section 55(2)(a).....	59
section 40(4).....	264, 265, 294	section 55(2)(b).....	59
section 41.....	241, 261, 268, 294, 320	section 56.....	359
section 42.....	241, 260, 263, 284, 296, 298, 301, 320, 325, 326, 327, 345	section 56(1).....	353
section 42(a).....	297	section 56(2).....	353
section 42(b).....	297	section 56(3).....	359
section 42(c).....	298	section 56(4).....	354, 359
section 42(d).....	299	section 56(5).....	354, 359
Part 3.....	300	section 57(1).....	354
section 43.....	260, 263, 282, 284, 300, 325, 327	section 57(2).....	354
section 43(1).....	300, 302	section 58.....	354
section 43(1)(a).....	300, 301	section 59.....	354
		section 59(2).....	354
		section 59(3).....	355

section 59(4) .....	355	section 72(4) .....	362
section 59(5) .....	355	section 72(6) .....	362
section 60 .....	355	section 73 .....	362
section 61 .....	366	section 74(1) .....	362
section 61(1) .....	355	section 74(2) .....	362
Part 4 .....	349, 353, 355	section 74(4) .....	362
section 62 .....	350	section 74.5 .....	353
section 62(1) .....	364	section 75 .....	365, 366
section 63 .....	30, 351	section 75(2) .....	366
Part 5 .....	45, 355	section 76 .....	366
section 65 .....	90, 96, 355, 363	section 79(1) .....	365
section 65(1) .....	76, 78, 91, 222, 231, 355	section 80 .....	39
section 65(2) .....	356	section 81(2) .....	45
section 65(3) .....	356, 363	section 81(6) .....	366
section 65(4) .....	356	section 82 .....	43, 44, 45, 353
section 65(5)(b) .....	199	section 82(1) .....	43
section 66 .....	356	section 82(2) .....	43, 352, 353
section 66(2) .....	216	section 82(3) .....	43, 353
section 66(2)(a) .....	357, 364	section 82(4) .....	44
section 66(2)(b) .....	357, 364	section 82(5) .....	44, 353
section 67 .....	362	section 82(6) .....	44, 353
section 67(1) .....	357	section 82(7) .....	43, 353
section 67(1)(a)(ii) .....	115, 213	section 83 .....	39-40, 72, 115, 217
section 67(2) .....	357	section 84 .....	35, 36, 79, 115, 211, 265, 357
section 68 .....	358	section 84(1) .....	35, 40, 270
section 69 .....	353, 359	section 84(1)(a) .....	36
section 69(1) .....	358	section 84(1)(b) .....	36
section 69(2) .....	359	section 84(1)(c) .....	36-37
section 69(3) .....	359	section 84(1)(d) .....	37
section 69(4) .....	359	section 84(1)(e) .....	37-39
section 69(5) .....	359	section 84(1)(f) .....	339
section 69(6) .....	360	section 84(2) .....	40
section 70 .....	358, 364	section 85 .....	27-28
section 70(a) .....	359	section 86 .....	29
section 70(b) .....	360	section 87 .....	29
section 71 .....	360	section 87(1) .....	41
section 71(1) .....	361	section 87.1 .....	41-42, 323
section 71(2) .....	361	section 87.1(1) .....	309
section 71(3)(a) .....	361	section 87.1(2) .....	309, 323
section 71(3)(b) .....	361	section 87.1(2)(d) .....	261, 266, 272, 296, 303
section 72 .....	45, 361, 362	section 87.1(3) .....	41, 266, 323
section 72(3) .....	350, 362	section 87.1(3)(a) .....	323
section 72(3)(b) .....	67	section 87.1(3)(b) .....	323
section 72(3)(c) .....	78	section 87.1(4) .....	41, 303, 323
		section 87.1(5) .....	41
		section 88 .....	301



section 88(1) .....	32
section 88(2) .....	32
section 89(1) .....	31, 42-43, 186
section 89(2) .....	43
section 90 .....	44
section 91 .....	44
section 91(1) .....	45, 45
section 91(2) .....	45
section 92 .....	44-45, 355
section 92(1) .....	45, 299, 339
section 92(1)(e) .....	45, 71
section 92(1)(g) .....	71, 94
section 92(2) .....	45, 339
section 92(3) .....	44
section 93 .....	73, 79, 356
section 93(1) .....	73
section 93(2) .....	73
section 93(3) .....	73, 75
section 93(3.1) .....	50, 73, 77
section 93(4) .....	73, 74, 75, 77, 78
section 93(4.1) .....	73, 77
section 93(4)(a) .....	78
section 93(4)(b) .....	79, 80, 121, 230
section 93(5) .....	77
section 93(6) .....	73
section 95(a) .....	23
section 95(b) .....	73

### ***Freedom of Information and Protection of Privacy Regulation***

Schedule 1 .....	2, 16, 25, 29, 177, 182, 305, 307, 308, 309, 311, 313, 315
Schedule 2 (Fee Schedule) .....	56, 73, 74, 75, 83
Schedule 3 (Notice of Disclosure) .....	231
section 1(4) .....	173
section 3 .....	60
section 3(3) .....	61
section 4 .....	49, 91
section 5 .....	49
section 6 .....	138, 285
section 6(5) .....	138
section 7 .....	114, 261, 269, 270, 325
section 7(5) .....	262, 269
section 7(6) .....	262, 269
section 8 .....	280

section 9 .....	299, 301, 326
section 11 .....	49
section 11(4) .....	73
section 12 .....	49, 74
section 12(2) .....	57
section 13 .....	75
section 13(3) .....	54
section 14(1)(a) .....	76
section 14(1)(b) .....	76
section 14(2) .....	76
section 14(3) .....	76
section 15 .....	20
section 17 .....	20
section 18 .....	173, 174
section 18(1) .....	174





# **INFORMATION AND PRIVACY COMMISSIONER'S ORDER AND INVESTIGATION REPORT CITATIONS INDEX**



## Information and Privacy Commissioner's Order and Investigation Report Citations

Adjudication Order No. 2 .....	78	Investigation Report F2003-IR-001 .....	363
Adjudication Order No. 3 .....	203, 204	Investigation Report F2003-IR-002 .....	265
Adjudication Order No. 4 .....	130	Investigation Report F2003-IR-003 .....	259
Decision Regarding Section 70 of the <i>FOIP Act</i> , August 2003 .....	360	Investigation Report F2003-IR-004 .....	353
Investigation Report 98-IR-003 .....	239	Investigation Report F2003-IR-005 .....	237, 244
Investigation Report 98-IR-009 .....	69, 219, 315	Investigation Report F2004-IR-001 .....	233
Investigation Report 98-IR-011 .....	28, 29, 226, 227 228	Investigation Report F2004-IR-002 .....	265, 294
Investigation Report 98-IR-015 .....	275	Investigation Report F2005-IR-001 .....	363
Investigation Report 99-IR-001 .....	13	Investigation Report F2007-IR-004 .....	147
Investigation Report 99-IR-003 .....	311	Order 96-002 .....	78, 79
Investigation Report 99-IR-004 .....	51	Order 96-003 .....	99, 106, 137, 148, 188
Investigation Report 99-IR-005 .....	276	Order 96-004 .....	164
Investigation Report 99-IR-007 .....	238	Order 96-006 .....	145, 179, 180
Investigation Report 99-IR-008 .....	273	Order 96-007 .....	282
Investigation Report 99-IR-009 .....	28	Order 96-008 .....	130
Investigation Report 2000-IR-001 .....	65, 66	Order 96-011 .....	226, 229, 232
Investigation Report 2000-IR-002 .....	240	Order 96-012 .....	177, 188
Investigation Report 2000-IR-003 .....	270	Order 96-013 .....	101, 102, 104, 108, 188, 191
Investigation Report 2000-IR-004 .....	249	Order 96-014 .....	51, 229
Investigation Report 2000-IR-006 .....	257	Order 96-015 .....	354
Investigation Report 2000-IR-007 .....	249	Order 96-017 .....	86, 98, 197, 201, 203, 204
Investigation Report 2000-IR-009 .....	363	Order 96-018 .....	103, 107, 191
Investigation Report 2001-IR-001 .....	72	Order 96-019 .....	86, 145, 202, 211
Investigation Report 2001-IR-002 .....	264	Order 96-020 .....	17, 197, 200
Investigation Report 2001-IR-004 .....	51, 89	Order 96-021 .....	197, 202, 315
Investigation Report 2001-IR-005 .....	275	Order 96-022 .....	52, 71, 315
Investigation Report 2001-IR-006 .....	181, 247, 286 287	Order 97-002 .....	115, 116, 128, 130, 134
Investigation Report 2001-IR-010 .....	46, 53	Order 97-003 .....	18, 55, 198
Investigation Report F2002-IR-001 .....	121	Order 97-005 .....	192
Investigation Report F2002-IR-005 .....	265	Order 97-006 .....	51, 52, 69
Investigation Report F2002-IR-006 .....	119	Order 97-007 .....	16, 179
Investigation Report F2002-IR-007 .....	241	Order 97-008 .....	10
Investigation Report F2002-IR-009 .....	145, 236	Order 97-009 .....	6, 199, 202, 203, 226
Investigation Report F2002-IR-010 .....	238	Order 97-010 .....	167, 169, 170, 173
Investigation Report F2002-IR-012 .....	238, 239	Order 97-011 .....	130
		Order 97-013 .....	103
		Order 97-017 .....	16, 199
		Order 97-018 .....	213, 229
		Order 97-019 .....	54, 75, 315

Order 97-020.....84, 85, 254, 255, 256, 315

Order 98-001.....129, 254, 290, 362

Order 98-002.....32, 50, 51, 64, 238, 239, 251, 252

Order 98-003.....70, 315

Order 98-004.....36, 118, 125, 134, 198, 207

Order 98-005.....85, 192

Order 98-006.....102, 103, 191, 221, 222, 359

Order 98-007.....115, 132

Order 98-008.....102, 132, 211

Order 98-009.....92, 135

Order 98-010.....50, 254, 255, 256

Order 98-011.....79, 316

Order 98-012.....51, 52

Order 98-013.....17, 101, 111

Order 98-014.....117, 118

Order 98-016.....86, 202

Order 98-017.....199, 203, 228, 229

Order 98-018.....117, 118

Order 98-019.....17, 79, 229

Order 98-020.....96, 192

Order 98-021.....141, 142

Order 99-001.....178, 179

Order 99-002.....85, 167, 315

Order 99-005.....17, 198

Order 99-007.....104, 212

Order 99-008.....102

Order 99-009.....316

Order 99-010.....128, 150

Order 99-011.....49, 51, 52, 60, 360

Order 99-012.....46, 78

Order 99-014.....74, 80

Order 99-017.....104

Order 99-018.....105

Order 99-020.....8, 85

Order 99-021.....52, 62, 69, 71, 88, 315, 317

Order 99-023.....100, 218, 229, 356

Order 99-025.....9, 10, 285

Order 99-027.....21, 78, 201, 202

Order 99-028.....131, 132

Order 99-030.....218

Order 99-032.....7-8, 14, 275, 289

Order 99-033.....20, 100

Order 99-034.....20, 21

Order 99-035.....51, 53

Order 99-039.....52, 64, 78, 315

Order 99-040.....104, 168, 170, 178

Order 2000-003.....7, 12, 103, 109, 232

Order 2000-004.....92

Order 2000-005.....6, 7, 102, 104, 128, 129, 230

Order 2000-006.....99

Order 2000-007.....254, 256

Order 2000-008.....78

Order 2000-009.....105, 192

Order 2000-010.....105

Order 2000-011.....78

Order 2000-013.....17, 168, 169

Order 2000-014.....87, 91, 107, 222

Order 2000-015.....51, 92

Order 2000-016.....92

Order 2000-017.....102, 103, 104, 191, 229

Order 2000-019.....124, 134, 146, 198, 215

Order 2000-020.....13, 85, 312, 315

Order 2000-021.....51, 61, 97

Order 2000-022.....14, 52, 53

Order 2000-023.....13, 45, 69, 86, 124, 145

Order 2000-024.....14, 110

Order 2000-026.....130, 132

Order 2000-027.....145, 150

Order 2000-028.....86

Order 2000-029.....114, 132, 141

Order 2000-030.....45, 52, 69, 70, 316

Order 2000-031.....79, 229

Order 2000-034.....225

Order 2001-001.....86, 115, 134

Order 2001-002.....179, 180

Order 2001-004.....251, 255, 356

Order 2001-006.....162

Order 2001-007.....360

Order 2001-008.....102, 103, 104, 107, 168, 191

Order 2001-009.....207, 257

Order 2001-010.....103, 148, 275

Order 2001-011.....152

Order 2001-013.....31, 51, 52, 129, 147

Order 2001-014.....14

Order 2001-016.....84

Order 2001-018.....199

Order 2001-019.....103, 105, 107, 191

Order 2001-020.....117, 126

Order 2001-021.....	103, 110	Order F2003-017 .....	201, 203
Order 2001-023.....	79, 80	Order F2003-018 .....	98, 105, 128
Order 2001-025.....	199	Order F2003-019 .....	257
Order 2001-027.....	156	Order F2003-020 .....	53
Order 2001-029.....	13, 14		
Order 2001-030.....	152	Order F2004-005 .....	56
Order 2001-031.....	152	Order F2004-006 .....	102
Order 2001-032.....	354	Order F2004-010 .....	265
Order 2001-033.....	355	Order F2004-012 .....	192
Order 2001-034.....	241	Order F2004-013 .....	212
Order 2001-035.....	350	Order F2004-014 .....	115, 116, 118, 192
Order 2001-037.....	84, 164	Order F2004-015 .....	11, 126, 129, 174
Order 2001-038.....	261, 268, 295	Order F2004-016 .....	132
Order 2001-039.....	359	Order F2004-017 .....	230
Order 2001-040.....	174	Order F2004-018 .....	163, 164
Order 2001-041.....	53	Order F2004-021 .....	105, 179, 180
		Order F2004-022 .....	142, 195
Order F2002-002.....	102, 107, 110	Order F2004-023 .....	152
Order F2002-005.....	74	Order F2004-024 .....	113, 118, 263, 358
Order F2002-006.....	45, 113, 116, 233	Order F2004-026 .....	87, 116, 128, 130, 167, 168, 180, 181, 182
Order F2002-007.....	203	Order F2004-027 .....	253
Order F2002-008.....	143	Order F2004-028 .....	126
Order F2002-010.....	128, 132	Order F2004-029 .....	137
Order F2002-011.....	119	Order F2004-030 .....	230
Order F2002-012.....	11	Order F2004-032 .....	154, 155
Order F2002-014.....	69		
Order F2002-015.....	56	Order F2005-001 .....	132, 155
Order F2002-017.....	84	Order F2005-002 .....	277
Order F2002-018.....	270, 276	Order F2005-003 .....	239
Order F2002-020.....	363	Order F2005-004 .....	183
Order F2002-023.....	42, 45, 207	Order F2005-007 .....	21
Order F2002-024.....	145, 147	Order F2005-008 .....	254
Order F2002-025.....	89	Order F2005-009 .....	147
Order F2002-027.....	141	Order F2005-010 .....	15
		Order F2005-011 .....	105
Order F2003-001.....	52	Order F2005-012 .....	178
Order F2003-002.....	116, 117	Order F2005-013 .....	147
Order F2003-004.....	103, 113, 362	Order F2005-014 .....	270, 294
Order F2003-005.....	125, 126, 150, 199	Order F2005-016 .....	115, 116, 124, 128, 129, 130, 362
Order F2003-007.....	142	Order F2005-026 .....	152
Order F2003-008.....	252	Order F2005-030 .....	111, 201
Order F2003-009.....	103		
Order F2003-010.....	137	Order F2006-001 .....	77
Order F2003-011.....	79, 80	Order F2006-003 .....	37
Order F2003-014.....	179	Order F2006-004 .....	237
Order F2003-016.....	179, 180		



Order F2006-005.....	152
Order F2006-007.....	116, 117, 126, 130, 133, 192
Order F2006-008.....	116, 117, 126, 130, 133, 192
Order F2006-010.....	229, 232
Order F2006-012.....	92, 158, 355
Order F2006-013.....	158
Order F2006-015.....	158
Order F2006-016.....	363
Order F2006-017.....	256
Order F2006-019.....	249
Order F2006-023.....	192
Order F2006-025.....	142
Order F2006-028.....	58
Order F2006-030.....	116, 134
Order F2006-032.....	79
Order F2007-005.....	150, 154
Order F2007-007.....	130
Order F2007-008.....	133
Order F2007-013.....	87, 167
Order F2007-014.....	198, 230
Order F2007-015.....	117, 128
Order F2007-016.....	78
Order F2007-017.....	60
Order F2007-019.....	356
Order F2007-020.....	80
Order F2007-021.....	153
Order F2007-022.....	181
Order F2007-025.....	117, 119, 120, 128, 198, 201
Order F2007-028.....	51, 52, 315
Order F2007-029.....	70, 116
Order F2008-008.....	179, 180
Order F2008-009.....	124, 126, 134
Order F2008-010.....	116, 118, 126, 130, 134
Order F2008-012.....	130, 132, 133, 201
Order F2008-014.....	126, 127, 128
Order F2008-015.....	126, 127, 128
Order F2008-019.....	103, 106, 116
Order F2009-002.....	135

**WORDS AND PHRASES  
DEFINED OR DISCUSSED  
INDEX**



## Words and Phrases Defined or Discussed

ability to manage the economy .....	189	benefits (derived from research) .....	298
aboriginal organization .....	162	biometric information .....	7, Appendix 1
aboriginal people.....	132, 248	breach (security) .....	339
access .....	Appendix 1	burden of proof .....	Appendix 1
accurate .....	251	bylaw .....	172
active dissemination.....	32, Appendix 1	Cabinet.....	Appendix 1
activity of a public body (collection of personal information for) .....	237	case-by-case privilege.....	200
adjudicative function.....	184	claims, disputes or grievances .....	132, 248
adjudicator .....	365, Appendix 1	classify .....	115
administration of a public body .....	181-182	clearly in the public interest.....	121, 229
administration of personnel .....	247, 287	collected for the purpose of collecting a tax .....	110
administrative investigation .....	146	collected for the purpose of determining tax liability .....	110
adult interdependent partner .....	290	collection.....	236
advice .....	166, 179, Appendix 1	commercial activity.....	118
advice or recommendations (to Cabinet or Treasury Board) .....	166	commercial information.....	102, 191, Appendix 1
after giving notice .....	215	Commissioner.....	Appendix 1
agreement (under an enactment).....	270	committee of a governing body .....	173
allied state .....	149	committees of the Executive Council .....	166
analyses or policy options.....	179	committees of the Treasury Board.....	166
annotate (correction of personal information) .....	255	common interest privilege .....	199
applicant.....	49, Appendix 1	common or integrated program or service .....	262
applicant's rights.....	131	compelling circumstances (disclosure of personal information).....	115
arbitrator .....	109	compile (personal information).....	261, 268
archives of a public body .....	282, 300	complaint .....	Appendix 1
arrangement (under an enactment).....	271	complete information.....	251
assignee.....	263	comply with a treaty, arrangement or agreement.....	271
assist in resolving a problem (disclosure to MLA).....	281	comply with an enactment .....	270, 272
associated state.....	149	confidential source.....	150, Appendix 1
audit .....	183, 195, Appendix 1	confidentiality (condition of research agreement).....	298
audit purposes .....	281	consent in the prescribed manner.....	261
authorized disposition (of records) .....	310	consistent use (personal information) .....	261
authorized (by an enactment).....	272, 273	consistent purpose.....	246
Auditor General .....	279	constituency records .....	15
available for purchase by the public .....	207	consultation.....	180, Appendix 1
background facts .....	169	continuing request.....	Appendix 1
background research .....	185	contract to supply goods and services.....	118
bad faith .....	44	contracts.....	141
bargaining agent.....	281	control (of records) .....	6, 7, 254, Appendix 1
benefit .....	119	correctional record .....	155
benefits (confidential evaluations relating to award) .....	141		

created by or for.....	16	Executive Council.....	166
criminal intelligence .....	145, 151	exercise of discretionary power .....	184
Crown privilege .....	200	explicitly in confidence.....	104
Crown records (privileged information) .....	200	explicitly revealing (third party business	
custody (of records) .....	6, 7, 254, Appendix 1	information) .....	101
damage (to historic resources, vulnerable		explicitly reveals (Executive Council	
forms of life) .....	206	deliberations).....	167
damage the reputation .....	134	expressly authorized by an enactment	
data linkage .....	343	(collection of personal information).....	236-237
data matching .....	343, Appendix 1	extension .....	Appendix 1
data profiling.....	343	factual information (about an individual) .....	254
data sharing .....	343	fair.....	132
day of response .....	68	fair determination of rights .....	131
debt .....	244, 277	fair trial .....	153
decision that directly affects the individual .....	251	fees.....	Appendix 1
defence of Canada.....	149	fifteen (15) years.....	168
delegation.....	Appendix 1	financial details (of a contract) .....	118
deliberation(s).....	167, 173, 180	financial information.....	103, 191
details (of a discretionary benefit) .....	119	financial interests .....	189
disclose .....	265	financial loss .....	192
disclosure .....	Appendix 1	fine .....	244, 277
disclosure for audit purposes .....	Appendix 1	five (5) years .....	170
discretion.....	Appendix 1	FOIP.....	Appendix 1
discretionary (benefit).....	119, Appendix 1	FOIP Coordinator .....	Appendix 1
discretionary benefit of a financial nature.....	119	for (created by or for).....	16, Appendix 1
discretionary exception .....	97, Appendix 1	foreign state .....	162
draft.....	172	formal (research or audit report).....	183
draft legislation or regulations .....	166	frivolous .....	58
earliest reasonable time.....	298	gathered for the purpose of collecting a tax.....	127
economic interests.....	188	genetic information.....	7
educational body .....	2-3, Appendix 1	good faith.....	43
educational history .....	126	governing body (of a local public body).....	15, 173
elected officials (of a local public body).....	173	governing body (of a post-secondary	
electronic records.....	307	educational body).....	15
eligibility.....	125, 279	Government of Alberta (intergovernmental	
employee.....	115, 275, Appendix 1	relations, economic interests).....	162, 189
employment (confidential evaluations).....	141	Government of Alberta (non-arm's length	
employment history .....	126	transaction).....	111
employment responsibilities .....	116	grant (discretionary benefit).....	119
enactment.....	236, Appendix 1	guardian .....	Appendix 1
endangered form of life.....	206	guardian of a minor.....	38
error (in personal information).....	254	harm.....	99, Appendix 1
espionage .....	149	harm (intergovernmental relations).....	162
ethnic origin .....	129	harm (law enforcement).....	148
every reasonable effort.....	50, 64, 251	harm (record linkage).....	297
exceptions to disclosure .....	Appendix 1	harm significantly .....	106

- harm to health ..... 228
- harm to safety ..... 228
- harm to the environment ..... 228
- harm(s) test ..... 99, Appendix 1
- has been implemented ..... 170
- has been made public ..... 169
- head ..... 23, Appendix 1
- health care body ..... 3, Appendix 1
- historic resources ..... 206
- history (of an individual in the control  
of a correctional authority) ..... 156, 245
- identifiable individual ..... 233
- identity (of a confidential source) ..... 150
- immediate and grave harm ..... 138
- imminent danger ..... 292
- impartial adjudication ..... 153
- implementation ..... 182
- implicitly in confidence ..... 104, Appendix 1
- implicitly reveal (third party business  
information) ..... 101
- implicitly reveals (Executive Council  
deliberations) ..... 167
- imposed under a statute or regulation ..... 145
- in a reasonable manner (use and  
disclosure of personal information) ..... 264
- in camera ..... Appendix 1
- in confidence ..... 104, 163, Appendix 1
- in the absence of the public ..... 174
- inaccurate information ..... 250
- incomplete (research or audit report) ..... 183
- individually identifiable form (personal  
information) ..... 297
- information collected on a tax return ..... 109
- information ..... 226
- inquiry ..... Appendix 1
- interfere with ..... 152
- interfere with contractual or other negotiations ... 192
- interference with public safety ..... 137
- international organization of states ..... 162
- intervenor ..... Appendix 1
- investigation ..... 145, Appendix 1
- investigative techniques and procedures ..... 150
- judicial administration record ..... 9, Appendix 1
- judicial or quasi-judicial capacity ..... 9-10
- judicial review ..... 364, Appendix 1
- labour relations information ..... 103, Appendix 1
- labour relations officer ..... 109
- law enforcement ..... 124, 145, 237, 282, Appendix 1
- law enforcement agency ..... 282
- law enforcement investigation ..... 145
- law enforcement proceeding ..... 283
- law enforcement record ..... 124, 157
- lawfully detained ..... 154
- lead or could lead ..... 145
- legal advice ..... 197
- legal authority (for collection of  
personal information) ..... 248
- legal privilege ..... 197, Appendix 1
- legal proceedings ..... 5, Appendix 1
- legal services ..... 201
- legislative authority ..... 284
- licence ..... 118, Appendix 1
- link (correction of personal information) ..... 255
- litigation privilege ..... 198
- local government body ..... 3-4, Appendix 1
- local public body ..... 2, Appendix 1
- management of  
personnel ..... 181, 247, 286, Appendix 1
- mandatory exception ..... 96, Appendix 1
- matter of public interest ..... 115
- mediation ..... Appendix 1
- mediator ..... 109
- meeting ..... Appendix 1
- meeting (of a local public body) ..... 172
- Member of the Executive Council ..... 275
- Member of the Legislative Assembly ..... 280
- mental health ..... 137
- Minister responsible for the Act ..... Appendix 1
- monetary value ..... 191
- necessary for (an operating program) ..... 237
- necessary for (performing statutory duties  
or operating a program) ..... 285
- non-arm's length transaction (business  
information of a third party) ..... 111, Appendix 1
- non-arm's length transaction (record of a  
treasury branch, credit union) ..... 17, Appendix 1
- not be harmful ..... 298
- not contrary to the public interest .... 121, Appendix 1
- notice ..... Appendix 1
- offence ..... Appendix 1
- offence under an Act of Canada ..... 157
- office (of a district registrar) ..... 14



officer (of a public body).....	275	privacy impact assessment.....	328, Appendix 1
Officer of the Legislature.....	288, Appendix 1	privacy protection.....	234
omission (in personal information).....	252	private records.....	300
operating program.....	237	procedures, criteria, instructions and considerations.....	181
operating a program of a public body.....	277	proceeding(s).....	147, 283, 354, Appendix 1
opinions (about an individual).....	254	progress (on a report).....	183
order (of the Commissioner).....	Appendix 1	prohibition on subsequent use or disclosure.....	299
order (court).....	274	prior to giving notice.....	215
organized criminal activities.....	151	proposals.....	179
other benefits (confidential evaluations relating to award).....	141	proprietary interest.....	191, Appendix 1
other details (of a contract).....	118	prosecutorial discretion.....	152
other legal instrument (by which a local public body acts).....	172	protection of the environment.....	131
other persons or bodies (labour relations).....	109	public body.....	2, Appendix 1
other public sources (indirect collection of personal information).....	243	public event or activity.....	122, Appendix 1
other similar discretionary benefit.....	119	Public Guardian.....	246
paramourcy.....	Appendix 1	public health.....	130
parliamentary privilege.....	199	public interest, not contrary to (disclosure of personal information).....	121, Appendix 1
participant (in employee evaluation process).....	142	public interest (disclosure).....	79, Appendix 1
peace officer.....	153, Appendix 1	public interest (excusing fees).....	75, Appendix 1
penalty or sanction.....	145, Appendix 1	public interest (research).....	298
permit.....	118	public safety.....	130-131
person.....	153, Appendix 1	public scrutiny.....	130
person acting in judicial or quasi-judicial capacity..	9	Public Trustee.....	246
personal information.....	6-7, 56, 254, Appendix 1	published.....	208
personal information bank.....	41, Appendix 1	published sources (indirect collection of personal information).....	243, 260
personal note.....	9	purpose (collection of personal information).....	248, 260, 268
personal records.....	14	purpose (use of personal information).....	260
personal representative.....	Appendix 1	quality assurance committee.....	Appendix 1
personal service (of a notice).....	39	quasi-judicial body.....	285
physical health.....	137	racial origin.....	128
police informer privilege.....	199	range (salary).....	116
police investigation.....	146	rare form of life.....	206
policing.....	145, Appendix 1	readily available to the public.....	207
policy considerations.....	166	reasonable.....	Appendix 1
positions and plans.....	181	reasonable and direct connection.....	295
possession (of records).....	7	reasonable expectation of harm.....	Appendix 1
post-secondary educational body.....	11	reasonable security arrangements (for personal information).....	259, 335
power of attorney.....	34	reasons for decision.....	184
prejudice (to national security).....	149	recommendations.....	166, 179
prejudice to competitive position.....	192	record.....	6, Appendix 1
prescribed.....	261, Appendix 1	records.....	226, 265
presumed.....	123		
presumption.....	Appendix 1		

record linkage .....	297	settlement negotiation privilege .....	201
record made from information in a		severing .....	Appendix 1
Land Titles Office .....	14	significant harm .....	214
record of a credit union .....	17	solicitor-client privilege .....	197
recorded (personal information) .....	265	spouse .....	296
records retention and disposition		statement made during an inquiry .....	354
schedule .....	Appendix 1	statistical research .....	296
registrar .....	13	statistical survey(s) .....	185, Appendix 1
registry .....	14	statistics .....	185
related to a public body .....	122	statutory privilege .....	201
relates (to eligibility criteria) .....	125	subpoena .....	273
relates directly to (an operating program) .....	237	substance .....	167, 172
relations (intergovernmental) .....	162	substance of deliberations .....	Appendix 1
relationship of interdependence .....	291	substitutional service .....	40
relative .....	291	suitability .....	279
release (from a correctional institution) .....	245	supervision (by a correctional	
released to the public .....	208	authority) .....	156, 245, 289
relevant and material (correction of		systematic .....	57, 58
personal information) .....	256	teaching materials .....	11
relevant circumstances (unreasonable		technical information .....	104, 191, Appendix 1
invasion of privacy) .....	129-130	test .....	195
religious or political beliefs or associations .....	129	third party .....	102, 113, 211, Appendix 1
removal or destruction of individual identifiers .....	298	threat to availability of information .....	341
repetitious .....	57	threat to the confidentiality of information .....	341
report (labour relations) .....	109	threat to the integrity of information .....	341
representations .....	359	threaten .....	137
require .....	270, 272	threatened form of life .....	206
request .....	254, Appendix 1	time limit .....	Appendix 1
research information (post-secondary		trade secret .....	102, 190, Appendix 1
educational body employees) .....	12	transfer .....	Appendix 1
research purpose(s) .....	296	transitory record .....	312, Appendix 1
resolution (of a local public body) .....	172	Treasury Board .....	166
responsive records or information .....	Appendix 1	treaty .....	271
retain (personal information) .....	252	unfairly (damage to reputation) .....	134
review (by Commissioner) .....	356, Appendix 1	unreasonable interference with the	
risk of harm (public interest disclosure) .....	228	operations of a public body .....	58
routine disclosure .....	31, Appendix 1	use (of personal information) .....	260
routine inspections .....	157	validating .....	132, 248
sabotage .....	149	vexatious .....	58, 59
safety .....	137	voluntary .....	116
salary .....	116	volunteer .....	116
scientific information .....	103, 191, Appendix 1	vulnerable form of life .....	206
security .....	155, 298	waiver of privilege .....	203-204
security investigation .....	146	warrant .....	273
serious and repetitive criminal activities .....	151	without delay .....	226
service in electronic form .....	40	written authorization .....	38



## **SUBJECT INDEX**



# SUBJECT INDEX

## A

### **Abandonment of Request**

(*Model Letter F*) ..... 81, Appendix 3

### **Aboriginal Relations, see Alberta Aboriginal Relations**

### **aboriginal organizations**

intergovernmental relations ..... 161, 162, 163

### **aboriginal people**

claims, disputes or grievances ..... 129, 132, 248  
negotiations ..... 162

### **absenteeism reports** ..... 127

### **academic councils** ..... 15, 173

### **Access and Privacy** ..... 25

adjudication and adjudicators ..... 366  
consultation ..... 21, 357  
Directory of Public Bodies ..... 30  
FOIP request coordination ..... 62-63  
responsibilities ..... 29-30  
tracking system ..... 30, 61  
training ..... 30

### **Access Request Processing**

*Summary Form* ..... 82, Appendix 5

### **Access Request Recommendation**

*Form* ..... Appendix 5

### **Detailed Review of Records Form** ..... Appendix 5

### **access requests**

adequacy of search 50-51, 52, 69-70, 314-317, 360  
consultations  
    third parties ..... 211-212  
correction of personal information ..... 253-55  
disregarding ..... 58, 354  
    time limits ..... 59  
documenting ..... 82  
duty to assist ..... 50-51, 350, 356, 362  
evading ..... 45  
failing in duties ..... 78  
forms ..... Appendix 5  
notices ..... 39-40  
personal information ..... 51, 267  
processing ..... 68-94  
prosecutions ..... 158  
records excluded from *FOIP Act* ..... 91  
records issues ..... 314-317  
refusal of access ..... 1, 86, 88, 91  
refusal to confirm or deny existence  
    of records ..... 89  
responding to ..... 48-95, 88-92  
severing ..... 85-89

**access rights** ..... 1, 95, 98, 234

abuse ..... 57  
defined ..... 47  
limitations on ..... 95

**access to information** ..... 47-94

existing procedures ..... 5, 58  
methods ..... 47-94  
service in electronic form ..... 40

**Access to Information Act (Canada)** ..... 5, 21

**accountability** ..... 1, 130

accuracy, *see* **personal information, accuracy**

### **Acknowledgement of Receipt of Correction**

*Request (Model Letter S)* ..... 258, Appendix 3

### **Acknowledgement of Request**

(*Model Letter A*) ..... 53, 54, 55, 60, 63, Appendix 3

**active dissemination** ..... 33-35, 207-208

communications ..... 34  
copies of records ..... 88  
delegation of authority ..... 34-35  
Internet ..... 33  
records management ..... 313-314

activities, *see* **public events**

### **Acts of Alberta**

collecting personal information ..... 236  
disclosing personal information ..... 115, 270, 272  
disclosing third party information ..... 111  
prohibiting disclosure ..... 354  
restrictions ..... 302-303  
routine disclosure ..... 32

### **Acts of Canada**

collecting personal information ..... 236  
disclosing personal information ..... 115, 270, 272  
    restrictions ..... 302-303  
disclosing third party information ..... 111  
offences ..... 157  
prohibiting disclosure ..... 354  
routine disclosure ..... 32

### **addresses**

personal information ..... 6

**adequate search for records** ..... 51, 52-53, 69-70, 314-317, 360

**adjudication and adjudicators** ..... 360-366

Access and Privacy ..... 366

*FOIP Act* ..... 365-366

impartiality ..... 153

judgments

    reasons for decision ..... 184

routine disclosure ..... 33



- administration**
  - public bodies plans ..... 181-182
  - of personnel ..... 247, 286
- administrative investigations** ..... 125, 145-147
- Administrative Procedures Act*** ..... 9
- administrative proceedings**
  - law enforcement ..... 147
- administrative records** ..... 8, 11
  - Administrative Records*
  - Disposition Authority* ..... 94, 308
- admissions**
  - nursing homes ..... 272
- Adult Guardianship and Trusteeship Act*** ..... 338
- adult interdependent partner** ..... 284, 290, 355
  - defined ..... 290-291
- Advanced Education and Technology, *see*
  - Alberta Advanced Education and Technology**
- advertising** ..... 312
- advice**
  - defined ..... 166, 179
  - Executive Council ..... 166-171
  - Information and Privacy Commissioner... 350, 352
  - legal matters ..... 197-198, 202, 274
  - officials ..... 177-187
  - records 15 years old ..... 183
- Affidavit for Witness Form*** ..... Appendix 5
- age**
  - personal information ..... 6
- agencies** ..... 2, 25
  - agenda or minutes ..... 182
  - intergovernmental relations ..... 161
- agenda**
  - consultations or deliberations ..... 180
  - Executive Council ..... 167, 168
  - in camera* meetings ..... 175
  - public bodies ..... 177, 182
- Agenda and Priorities Committee** ..... 166
- agents**
  - collection of personal information ..... 236
  - Personal Directives Act* ..... 36-37
- Agreement for Access to Personal Information for Research or Statistical Purposes Form*** ..... Appendix 5
- agreements**
  - disclosing personal information ..... 270-272, 296
  - contents of ..... 272, 296-297
  - research ..... 296-297
  - expert consultations ..... 285
  - law enforcement ..... 282-283
  - use of alumni records ..... 293
- Agriculture and Rural Development,
  - see* **Alberta Agriculture and Rural Development**
- air quality**
  - testing ..... 184
- Alberta Aboriginal Relations** ..... 30, 161, 163
- Alberta Advanced Education and Technology**.. 30
- Alberta Agriculture and Rural Development**.... 30
- Alberta Alcohol and Drug Abuse Commission** ..... 3
- Alberta (Attorney General) v. Krushell*** ..... 9
- Alberta Corporate Human Resources** .... 118, 172, 247, 286, 336
- Alberta Culture and Community Spirit** ... 30, 206
- Alberta Education** ..... 30
- Alberta Environment** ..... 30
- Alberta Evidence Act***
  - section 9 ..... 10
  - section 34 ..... 200
- Alberta Finance and Enterprise** ..... 278
- Alberta Health and Wellness** ..... 30, 56, 329
  - publications ..... 56, 57, 331, 336, 344
- Alberta Health Services** ..... 3, 18, 56
- Alberta Housing Act*** ..... 4
- Alberta Infrastructure** ..... 293
- Alberta International and Intergovernmental Relations** ..... 161, 163
- Alberta Justice and Attorney General** .... 246, 277, 285, 286
  - adjudication and adjudicators ..... 366
  - prosecutions ..... 152-153
  - protocols
    - disclosure of personal information ..... 228
- Alberta Labour Relations Board** ..... 10, 109, 153, 283, 285
- Alberta (Minister of Justice) v. Roy*** ..... 365
- Alberta Municipal Affairs** ..... 30
  - disclosure harmful to intergovernmental relations ..... 163
- Alberta Records Centre** ..... 8, 252, 315
- Alberta Records Management Committee** ..... 94, 253, 310
- Alberta Records Management Committee Circulars** ..... 310
- Alberta Rules of Court** ..... 286
- Alberta Seniors Benefit** ..... 245, 272
- Alberta Solicitor General and Public Security** ..... 30, 282, 289
- Alberta Transportation** ..... 157, 293
- Alberta Transportation Safety Board** ..... 285
- Alberta Treasury Branch** ..... 17
- alliances** ..... 148-149
- allocations (permits and licences)** ..... 119

- alumni records**  
 fund-raising..... 263-264, 293, 325  
 post-secondary educational bodies .... 263-264, 293
- analyses**  
 advice and recommendations..... 177, 178-180
- Annotation to Personal Information Form**..... 256, 257, 258, Appendix 5
- anonymizing (personal information)**..... 264
- appeal body**  
 Executive Council ..... 169
- applicants**  
 assisting ..... 24, 49-53, 83-84, 88-89, 350  
 burden of proof ..... 78, 360-361  
 harm to health or safety ..... 138, 285  
 identities ..... 69, 214, 219  
 notices ..... 219, 221  
 proof of identity ..... 35, 37, 38, 89  
 refusal to disclose own personal information ..... 138  
 responding to ..... 53, 88-92, 100, 350-357  
 rights ..... 87-88, 88-89, 95  
   determination of rights ..... 131-132  
   fee waivers ..... 78-79  
   reviews ..... 355-361  
 sophisticated ..... 50-51
- appointment books**  
 elected officials ..... 14
- arbitrators** ..... 108, 109  
 reports ..... 108, 109
- archaeological resources**..... 206
- archives**  
 church records ..... 12  
 disclosing business information..... 111  
 disclosing personal information to..... 282  
 disclosure of personal information ..... 300-302  
 information 25 years old ..... 301  
 labour union records ..... 12  
 member of Executive Council records ..... 12  
 policies and procedures ..... 302  
 post-secondary educational bodies ..... 300-302  
 private records ..... 12  
 records 75 years old ..... 301  
 records excluded from the Act..... 5, 12  
 transfer of records to ..... 71, 282, 303, 310, 315  
 unrestricted records ..... 300-302
- ARDA, see administrative records, Administrative Records Disposition Authority**
- ARMA** ..... 305
- arrangements**  
 disclosing personal information..... 270-272  
 law enforcement ..... 282-284
- assessment, see property assessment information**
- Assessment Review Boards** ..... 10  
 reasons for decision ..... 184
- assets**  
 public bodies..... 188  
 verification of ..... 245
- assistance, see duty to assist**
- associations**  
 personal information..... 6, 128-129, 233
- atmosphere**  
 harm to..... 228
- Attorney General, see Minister of Justice and Attorney General**
- audio tapes**..... 233
- audio visual recordings**..... 6
- Auditor General**..... 279  
 disclosing personal information to ..... 288  
 office..... 2  
 records ..... 8  
 records excluded from *FOIP Act*..... 10  
 reports ..... 229
- Auditor General of Canada** ..... 279
- audits**  
 Chief Internal Auditor, by ..... 19, 96, 186  
 confidentiality..... 105  
 disclosure of personal information for..... 280  
 electronic records..... 313, 335  
 for accuracy (personal information) ..... 251  
 harm to..... 195  
 health and safety ..... 105  
 incomplete reports ..... 183  
 Information and Privacy Commissioner, *see Information and Privacy Commissioner, audits*  
 methods and procedures ..... 195  
 personnel management ..... 195, 266  
 privacy ..... 332, 364  
 review ..... 116  
 routine disclosure..... 33  
 tax ..... 110
- Authorization of Representative Form**...Appendix 5
- authorized representatives**  
 disclosing personal information to ..... 35  
 written..... 39, Appendix 5
- awards**  
 receipt of..... 122-123  
 suitability for ..... 242-243
- B**
- background facts**  
 defined..... 169  
 Executive Council or Treasury Board ..... 168, 169-170

- not advice..... 179
  - reports to be published..... 207-208
  - records prepared for other uses..... 169
  - scientific..... 185
  - technical..... 185
  - bad faith**..... 44
  - bail**..... 154, 155, 156, 245, 289
  - bailiffs**..... 141
  - Banff Centre**..... 3
  - bank account**..... 124, 127
  - banking records**..... 17, 127
  - bankruptcy**..... 110
  - bargaining agents**
    - disclosing personal information to..... 181, 281
  - bargaining positions**..... 181
  - benefits**
    - confidential evaluations..... 141-142
    - continuing eligibility for..... 245-246
    - denying..... 263, 295, 346
    - eligibility..... 245, 286, 343
  - bills, drafts of**..... 182
  - biometric information**..... 7
    - collection..... 7
    - use..... 7
    - disclosure..... 7
  - blood type**..... 7
  - Board of Reference**..... 10
  - boards**..... 2, 17
    - agenda or minutes..... 182
    - appointees..... 116, 289
  - boards of governors**..... 15, 173
  - bombs**
    - technical information..... 155
    - threats..... 149, 228
  - bonding**..... 103
  - books**..... 6
  - briefing materials or notes**
    - briefing books or binder..... 18-19
    - Executive Council or Treasury Board..... 168
    - lawyer..... 196
    - Minister, for..... 18-19
  - brochures**
    - collection of personal information..... 249, 335
  - budgets**
    - pending decisions..... 177, 182-183
    - personnel..... 182
    - preparation documents..... 189
    - third parties..... 103
  - buildings, see property**
  - burden of proof**..... 360-361
    - confidential information..... 133, 164
    - disclosing personal information..... 360-361
    - exclusions from Act..... 14
    - third parties..... 360, 361
    - waiver of privilege..... 203
  - bursaries**..... 242
  - business contact information**..... 290
  - business plans**..... 103, 181-182, 191
  - Business Watch International Inc. v. Alberta***  
*(Information and Privacy Commissioner)* .... 360, 365
  - businesses**
    - budgets..... 103
    - client records..... 103
    - contracts..... 103
    - financial gain..... 108
    - financial loss..... 108
    - GST number..... 103
    - harm..... 101, 106-112
    - information
      - 50 years old..... 111
      - company history..... 107
      - revealed..... 101-104
    - licences and permits..... 118-119, 268
    - personnel management..... 103
    - records..... 101-104
    - tax information..... 109-110
  - bylaws**
    - considered enactments..... 236
    - drafts..... 172, 175-176
    - information readily available to public..... 207
    - law enforcement..... 146
    - personal information..... 125, 236
    - local public bodies..... 6, 172, 175-176
    - municipal..... 125, 172, 236
- C**
- Cabinet confidences**..... 166-171
    - records
      - 15 years old..... 168
      - 5 years old..... 170
  - Cabinet ministers, see ministers**
  - Cabinet documents**..... 355
  - Cabinet Policy Committees**..... 17, 166, 180
  - calendars**
    - elected officials..... 14
    - governing bodies..... 15
    - post-secondary educational bodies..... 249
  - campaign records** *see records, election campaign*
  - Canada Revenue Agency**
    - verification of income..... 254, 270
  - Canadian General Standards Board**..... 305
  - Canadian Security Intelligence Service**..... 164
  - Canadian Security Intelligence Services Act***  
*(Canada)*..... 147
  - case-by-case privilege**..... 200-201

- catalogues** ..... 207  
**'cc'-ing, see copying (on letters)**  
**Charitable Fund-raising Act** ..... 273  
**charter schools** ..... 3, 121  
**Checkstop programs** ..... 158  
**Chief Electoral Officer**  
   disclosing personal information to ..... 288  
   office ..... 2  
   records excluded from *FOIP Act* ..... 10  
**Chief Internal Auditor**  
   disclosure of audit information ..... 19, 96, 186  
   time limits ..... 19, 186  
**Chief Justice of Alberta** ..... 366  
**Child and Family Service Authorities** ..... 277  
   children, *see minors*  
**children's services** ..... 277  
**Child, Youth and Family Enhancement Act** ..... 21, 111  
**churches**  
   archival records ..... 12  
   membership ..... 129  
   civil actions, *see legal matters, civil legal cases*  
**civil liability**  
   discretionary exceptions ..... 156  
**class photographs** ..... 121, 249  
**class reunions** ..... 121  
**client records**  
   businesses ..... 103  
   economic interests of public bodies ..... 191  
   routine disclosure ..... 32, 33, 35  
**clients**  
   surveys ..... 249  
**collection agencies** ..... 278  
**collection of personal information** ..... 235-250, 302-303  
   agreements between public bodies ..... 236  
   best practices ..... 334-335  
   collecting fines or debts ..... 244  
   compliance reviews ..... 320  
   consent to indirect collection ..... 240-241  
   contracts and contractors ..... 235  
   correctional authorities or institutions ..... 244-245  
   direct ..... 240, 320-322  
   emergencies ..... 242  
   employees ..... 352-355  
   forms ..... 236, 333-335  
   from Internet ..... 243  
   from other public bodies ..... 241-242  
   fund-raising ..... 243, 325  
   honours or awards ..... 242, 343  
   indirect ..... 237, 240-248, 335, 345, 350  
   interviews ..... 236, 249  
   investigations ..... 243-244, 350, 360-364  
   law enforcement ..... 237, 243-244, 345  
   legal matters ..... 245  
   legal proceedings ..... 245  
   limitations on ..... 238-239  
   maintenance enforcement ..... 246  
   means of collecting ..... 236  
   methods ..... 240-248, 320-321  
   notices ..... 248-250, 321-322, 334  
     exceptions ..... 250  
   personnel management ..... 247-248  
   programs and services ..... 237-239  
   provision of legal services ..... 245  
   purposes ..... 234-235, 236-239, 260-261, 294-295  
   registries ..... 13-14  
   review of practices ..... 239  
   surveys ..... 236, 334, 363  
   unauthorized ..... 259, 353  
   verifying eligibility for programs  
     or services ..... 245-256  
   web sites ..... 334  
**collective agreements** ..... 103  
**College of Alberta Psychologists**  
   regulated member ..... 138  
**colleges** ..... 3, 126  
   enrolment ..... 121-122  
   governing body ..... 173  
   reunions ..... 121  
**colour**  
   personal information ..... 6  
**commercial activity** ..... 118  
**commercial information** ..... 102-103, 104, 190-191  
   Commissioner, *see Information and Privacy Commissioner*  
     **Commissioner**  
**commissions** ..... 2  
   agenda or minutes ..... 177, 182  
   police commissions ..... 174  
**committees**  
   appointees ..... 116  
   Cabinet ..... 166  
   governing bodies ..... 173  
   interdepartmental ..... 62  
**common interest privilege** ..... 199  
   common programs or services, *see programs and services, common programs*  
**communications**  
   Cabinet decisions ..... 169  
   information dissemination ..... 34  
   solicitor-client ..... 197-198  
   strategies ..... 26  
**communications systems**  
   security ..... 155  
**community health councils** ..... 3  
**community library boards** ..... 5



- community service work** ..... 156, 245, 289  
**competitive position**  
   harm..... 106-107  
   public bodies..... 191-192  
**complaints**..... 234, 350, 362-364  
   duty to assist ..... 350, 356, 362  
   extension of time limits ..... 215-216, 350, 356, 362  
   fees..... 350, 356, 362  
   investigations..... 362-364  
   law enforcement ..... 125, 148  
     investigations..... 125, 145  
   personal information correction..... 350, 356, 362  
   personal information banks ..... 41  
   public interest disclosure ..... 230  
   requesting a review..... 355-357  
   school board..... 276  
   time extensions ..... 67, 215-216  
   time limits..... 364  
**Computers for Schools** ..... 311  
**computers**  
   security ..... 259-260, 335-340, 340-342  
**Conducting Surveys: A Guide to Privacy Protection** ..... 334  
**confidential information**  
   Cabinet and Treasury Board ..... 166-171  
   Chief Internal Auditor  
     audit information ..... 19, 96, 186  
   complaints  
     law enforcement ..... 148  
   confidential sources ..... 150-151, 199-200  
   correctional records ..... 155-156  
   employment ..... 141-144  
   evidence of..... 105  
   Executive Council ..... 166-171  
   explicit ..... 104  
   home address ..... 134  
   identity of source  
     health or safety threats..... 139  
     law enforcement ..... 150-151, 199-200  
   implicit..... 104  
   intergovernmental relations ..... 163-164  
   law enforcement ..... 150-151  
   local public bodies..... 172-176  
     records 15 years old..... 175  
   solicitor-client communications..... 197-198  
   test for..... 104-106  
   third parties  
     private records ..... 200-201  
     third party business..... 40, 104-106  
     unreasonable invasion of privacy ..... 132-134  
   confidential sources, *see* **confidential information**, confidential sources  
     confidentiality clauses ..... 105  
**conflicts of interest**  
   Ethics Commissioner..... 11  
   Information and Privacy Commissioner ..... 356  
**Conflicts of Interests Act** ..... 11  
**conflicts of laws** ..... 20-21  
**consent**  
   absence of..... 263  
   collecting personal information..... 240, 245  
   disclosing confidential information  
     intergovernmental relations..... 164  
   disclosing personal information..... 114-115, 269-270, 281  
   disclosing third party information ..... 110, 220  
   disclosure harmful to intergovernmental relations..... 163  
   exercise by other persons..... 115  
   forms..... 261-262, 325, Appendix 5  
   using personal information ..... 261-263  
   written..... 261  
**conservation**  
   endangered forms of life..... 206  
   historic resources ..... 206  
**conservation officers** ..... 282  
   consistent purpose, *see* **personal information**, consistent use  
   consistent use, *see* **personal information**, consistent use  
**constituency records** ..... 15  
   consultants, *see* **contracts and contractors**  
**consultations**  
   economic interests of public bodies..... 189  
   FOIP requests ..... 62, 63, 71, 214  
   historic resources ..... 206  
   intergovernmental relations ..... 164  
   officials..... 180  
   privileged information..... 197  
   public bodies..... 214  
   stakeholder..... 180  
   third parties..... 65, 211-224  
     public interest..... 229-230  
**contaminants** ..... 227  
**contempt of court** ..... 273  
   Information and Privacy Commissioner... 353, 359  
**continuing FOIP requests** ..... 54-55  
   fee estimates ..... 54, 75  
   fees..... 54, 74  
   tracking..... 54  
**contracts and contractors**  
   administrative records ..... 8  
   advice and recommendations..... 178  
   audits ..... 280  
   collecting personal information ..... 235  
   commercial information ..... 103

- confidential evaluations ..... 141-144  
 confidentiality clauses ..... 105  
 data matching ..... 348  
 disclosing business contact information ..... 290  
 disclosing personal information ..... 114, 118, 126, 267-268  
 disclosure of personal information  
     to employees ..... 275  
 employment contracts ..... 115-117, 126, 141, 268  
*FOIP Act* ..... 8  
 goods and services ..... 118, 268  
 health care ..... 229  
 Information and Privacy Commissioner ..... 352  
 management of personnel ..... 247, 286  
 negotiations ..... 106-107, 181, 191  
 personal information ..... 114, 115, 116, 118, 268  
 personal information systems ..... 333  
 personal service contracts ..... 116, 118, 181, 244, 268  
 price ..... 103  
 privacy protection ..... 235  
 records ..... 8, 314  
     retrieval ..... 69  
     routine disclosure ..... 33  
     sending out to avoid *FOIP Act* ..... 45  
 research reports ..... 183  
 security ..... 339-340  
 terms and conditions of contracts ..... 115-118, 268  
 trade secrets ..... 102, 190  
**control (of records)** ..... 7-8  
     evidence for law enforcement ..... 125  
     law enforcement records ..... 147  
**coordinating committees**  
     information dissemination ..... 34  
**copying (on letters)** ..... 270  
*Copyright Act (Canada)*  
     section 32.1 ..... 21  
**Corporate Challenge** ..... 247  
**Corporate Chief Information Officer**  
     (Government of Alberta) ..... 329  
     policies ..... 202, 259, 311, 313  
 Corporate Human Resources, *see* **Alberta Corporate Human Resources**  
**corporations** ..... 2  
     agenda or minutes ..... 177  
     archival records ..... 12  
     banking records ..... 17  
     personal information, not ..... 113, 233  
     registry records ..... 13  
 correction of personal information,  
     *see* **personal information, correction**  
**correctional authorities or institutions**  
     collecting personal information ..... 244-245  
     disclosing personal information to ..... 288-289  
     escape from ..... 154  
     individuals under the supervision of ..... 155, 156  
     inmates  
         legal representatives ..... 292  
         records ..... 155-156  
**correctional officers** ..... 153  
**correspondence** ..... 6  
     copying ('cc') ..... 270  
     elected officials ..... 14  
     members of governing bodies ..... 15  
     Minister of Justice and Attorney General ..... 196, 201-202  
     ministers ..... 16-17, 168  
     MLAs ..... 16-17  
     Officers of the Legislature ..... 10-11  
     Secretary to Cabinet ..... 168  
**cost-benefit analysis**  
     data matching ..... 346  
**counseling records**  
     retention ..... 253  
**course evaluations**  
     post-secondary educational bodies ..... 293-294  
**Court of Appeal of Alberta**  
     excluded from *FOIP Act* ..... 4  
     records ..... 9  
**Court of Queen's Bench of Alberta**  
     excluded from *FOIP Act* ..... 4  
     judges ..... 365  
     judicial review ..... 364  
     records ..... 9  
**court administration records** ..... 6  
**court records** ..... 4, 9  
**credit card information** ..... 127  
*Credit Union Act*  
     records ..... 17-18  
     section 120(3) ..... 18  
**Credit Union Central Alberta Limited** ..... 17-18  
**Credit Union Deposit Guarantee Corporation** ..... 18  
**credit unions**  
     records ..... 17-18  
**crime prevention** ..... 151, 153-154, 158  
**Crimestoppers programs** ..... 158  
**criminal acts**  
     commission of ..... 151, 154  
     disclosure contrary to public interest ..... 120, 268  
     organized ..... 151  
     serious and repetitive ..... 151  
*Criminal Code (Canada)* ..... 125, 146, 152, 157  
**criminal history**  
     correctional records ..... 155-156  
     disclosure in public interest ..... 228, 229-230



personal information..... 7  
**criminal intelligence**..... 145, 151-152  
 criminal records, *see* **criminal history**  
**Crown Debt Collections**..... 278  
**Crown privilege**..... 200  
 CSIS, *see* **Canadian Security Intelligence Service**  
 Culture and Community Spirit, *see* **Alberta Culture and Community Spirit**  
**custodians**  
   data matching..... 344  
   privacy impact assessments ..... 328-329, 340, 344  
   security policy ..... 336  
**custody (of records)** ..... 7  
   law enforcement records..... 147, 153, 155  
 customer records, *see* **client records**

## D

damage, *see* **harm**  
**data**  
   encryption ..... 328, 339  
**databases**  
   information dissemination ..... 33  
   local public bodies ..... 33  
   matching ..... 297-298, 326-327, 343-348, 352  
   routine access..... 33  
   security ..... 348  
   sharing ..... 326-327, 329, 343-348  
 deaf, *see* **hearing-impaired persons**  
**debts**  
   collection of personal information..... 244  
   disclosure to collect ..... 277-278  
   securing ..... 13  
**deceased individuals**  
   disclosure not unreasonable invasion  
     of privacy ..... 290  
   disclosure of personal information ..... 284, 290  
   exercising rights of ..... 36, 356  
   more than 25 years deceased ..... 120, 268, 301  
   privacy ..... 120, 268  
   proof of death ..... 292  
   relatives ..... 284, 291, 356  
   reputation ..... 132  
**deemed refusal**..... 64  
**defence**  
   Canada ..... 148-149  
   international relations ..... 148  
**degrees**  
   honorary ..... 122, 242  
**delegation of authority**..... 27-29  
   routine disclosure ..... 27, 34-5  
**delegation instruments** ..... 24, 27-29  
**delegation tables**..... 28, Appendix 2

**deliberations**  
   officials ..... 180  
   substance of  
     Cabinet and Treasury Board..... 166-171  
     local public bodies..... 172, 173-175  
**Department of National Defence** ..... 162  
**dependent adults** ..... 246  
**Dependent Adults Act** ..... 273  
**deputy ministers**  
   disclosure statements ..... 11  
**design specifications**..... 104  
 detriment, *see* **harm**  
**development permits**..... 118  
 diagnostic and treatment information,  
   *see* **health care**, personal information  
**Developing Records Retention and Disposition Schedules** ..... 306, 310  
**diaries**..... 200  
 direct collection, *see* **personal information**,  
   direct collection; **collection of personal information**, direct  
**digital signatures** ..... 328, 335  
**Director of Maintenance Enforcement** ..... 246, 273, 287  
 directories, *see* **records**, directories of holdings;  
   **personal information banks**, directories;  
   **public bodies**, directory of  
**disabled persons**  
   FOIP requests ..... 49  
**disabilities**  
   personal information..... 7  
 disasters, *see* **emergency planning**  
**disclosure**  
   advice from officials..... 177-187  
   audit by Chief Internal Auditor ..... 19, 96, 186  
   business contact information ..... 130  
   by Information and Privacy  
     Commissioner ..... 354-355  
   communications strategies..... 26  
   emergencies ..... 115  
   employee information..... 115-117, 126, 127, 130, 141  
   exposure to civil liability ..... 156  
   extent of disclosure..... 294  
   harm to economic and other interests  
     of public bodies..... 188-194  
   harm to health or safety ..... 137-140  
   harm to historic resources..... 206  
   harm to intergovernmental relations..... 161-165  
   harm to law enforcement ..... 145-156  
   health or safety danger..... 115  
   notices ..... Appendix 3

- individual under supervision of
  - correctional authority ..... 155, 156
- information 25 years old ..... 301
- labour relations information ..... 108-109
- licences and permits ..... 118-119, 268
- mandated by Act or bylaw ..... 32
- negotiations ..... 181
- not unreasonable invasion of privacy ..... 113-123, 200-201, 251, 283
- oral disclosure ..... 105, 113
- personal information ..... 113-136, 264-296, 326
  - archival purposes ..... 282, 300-303
  - collecting fines or debts ..... 277-278
  - common programs and services ..... 276-277
  - compliance reviews ..... 319-327
  - compliance with enactments ..... 270-272
  - compliance with subpoena, warrant or order ..... 273-274
  - consent ..... 114-115, 269-270, 280
  - consistent use ..... 268
  - constraints
    - law enforcement ..... 282
  - constraints on ..... 264, 276, 268-269
  - contracts ..... 114-116, 118
  - correctional authorities or institutions. 154-156, 288-289
  - court proceedings ..... 285-286
  - deceased individuals ..... 290-292
  - defined ..... 265
  - discretionary benefits ..... 115, 117
  - emergencies ..... 115, 284, 285
  - enforcing legal rights ..... 277
  - expert consultations ..... 285
  - foreign courts ..... 44
  - for investigations ..... 125, 282-284
    - forms ..... Appendix 5
  - guardians ..... 36
  - Health Information Act*, subject to ..... 138
  - Internet ..... 265, 289
  - judicial tribunals ..... 285-286
  - labour unions ..... 281-282
  - law enforcement ..... 282-284
  - legal matters ..... 277
  - legal proceedings ..... 277, 282-284
  - maintenance enforcement ..... 246-247, 287
  - making payments ..... 277-278
  - minors ..... 37-39
  - not contrary to public interest ..... 268
  - notice ..... 218-219
  - Officers of the Legislature ..... 288
  - oral disclosure ..... 113
  - original and consistent use ..... 268-269
  - personnel management ..... 286-287
  - proof of identity ..... 35, 37, 38, 89
  - public events ..... 122
  - public health ..... 130-131
  - public information ..... 225-232, 289
  - public interest ..... 120-123
  - public safety ..... 130-131
  - public scrutiny ..... 130
  - quasi-judicial proceedings ..... 285-286
  - quasi-judicial tribunals ..... 285-286
  - record of purposes ..... 303-304
  - records of ..... 264-267
  - refusal of consent ..... 270
  - research agreements
    - contents of ..... 296
  - research purposes ..... 284, 296-297, 326
  - restrictions on archives ..... 298-299
  - statistical purposes ..... 296, 326
  - to avert imminent danger to
    - health or safety ..... 292
  - to bargaining agents ..... 281-282
  - to custodians under the
    - Health Information Act* ..... 138
  - to Information and Privacy
    - Commissioner ..... 43-44, 288, 352-353
  - to employees ..... 274-276
  - to ministers ..... 274-276
  - to MLAs ..... 280-281
  - to Ombudsman ..... 288
  - to Public Trustee ..... 246
  - to representatives ..... 36-39
  - unauthorized ..... 259-260, 266
  - use after disclosure ..... 241-242, 263
  - vehicle accidents ..... 293
  - verifying eligibility ..... 279
  - policies ..... 98
  - privileged information ..... 196-205
  - protection of environment ..... 130-131, 227, 228
  - public interest ..... 120-123, 204, 265
    - notices ..... 230-231
  - published information ..... 207-209
  - records excluded from *FOIP Act* ..... 18
  - research purposes ..... 284, 296-297, 326
  - tax information ..... 109-110, 127
  - third party business information consent ..... 110
  - third party personal information ..... 218-219
  - to Information and Privacy Commissioner 352-353
  - unreasonable invasion of privacy ..... 113-136
    - determining ..... 129-135
    - without delay ..... 226
  - discovery, *see examination for discovery*
  - discretion**
    - exercising ..... 97-98
    - fee waivers ..... 77

- discretionary benefits**  
 disclosure  
   not unreasonable invasion  
     of privacy ..... 115-117, 118-120, 267  
   employees ..... 115-117, 120, 267  
   settlement agreement ..... 120  
**discretionary exceptions** ..... 97  
 advice from officials ..... 177-187  
 civil liability ..... 156  
 confidential evaluations ..... 141-144  
 exercising of discretion ..... 97-98  
   advice from officials ..... 177-178  
 harm to economic and other interests  
   of public bodies ..... 188-194  
 harm to historic resources ..... 206  
 harm to law enforcement ..... 145-156, 302  
 harm to public or individual safety ..... 137-140  
 individual under supervision  
   of correctional authority ..... 155, 156  
 intergovernmental relations ..... 161-165  
 local public body confidences ..... 172-176  
 multiple ..... 100  
 notices ..... Appendix 3  
 privileged information ..... 196-205, 302  
 published information ..... 207-209  
 severing ..... 85-86  
**discretionary powers**  
 reasons for decision ..... 184  
 multiple reasons ..... 100  
**district registrars** ..... 13  
**Divorce Act (Canada)** ..... 38  
**DNA** ..... 7  
   *see also* inheritable characteristics  
**DNA Identification Act (Canada)** ..... 7  
**documentation**  
 line-by-line review of records ..... 82, 86-87  
**documents** ..... 6  
 creation for ease of severing ..... 87  
 drafts  
   transitory records ..... 310  
**Drainage boards** ..... 4  
**Drainage Districts Act** ..... 4  
**drawings** ..... 6  
**drugs**  
 criminal acts ..... 152  
**duty to assist** ..... 24, 32, 50-53, 84, 350, 356, 362  
 heads ..... 51  
 investigations ..... 362
- E**
- economic development agencies** ..... 162  
**economic interests**  
 harms test ..... 188-189  
 public bodies ..... 188-189  
**Edmonton Police Service v. Alberta**  
 (*Information and Privacy Commissioner*) ..... 360  
 Education, *see* **Alberta Education**  
**education**  
 personal information ..... 121-122, 126  
**educational bodies** ..... 2-3  
   *see also* **post-secondary educational bodies**  
   head ..... 23  
   tax information ..... 109-110  
   testing procedures ..... 195  
**educational history** ..... 7, 126  
**elected officials**  
 constituency records ..... 15  
 correspondence ..... 14  
 disclosing personal information about ..... 130  
 disclosing personal information to ..... 275-276  
 lawsuits ..... 130  
 meetings ..... 166-171, 173-175  
 personal records ..... 14  
**Election Act** ..... 288  
**elections**  
 local public bodies ..... 15  
**electoral information** ..... 288  
 electronic forms, *see* **forms, electronic**  
 electronic mail, *see* **records**  
**electronic records, see also records**  
 annotation ..... 255  
 audits ..... 313, 335  
 back-up ..... 52, 315  
 correcting ..... 255  
 creating new records form ..... 83-84  
 defined ..... 307  
 destruction ..... 311  
 disposition ..... 311  
 documentation ..... 316  
 management ..... 313-314  
 matching ..... 297-298  
 retrieval ..... 52, 69-70  
 records systems ..... 313  
 type of record ..... 6  
**electronic transactions (credit card)** ..... 127  
**Electronic Transactions Act** ..... 40  
 e-mail, *see* **records**  
**embarrassing information** ..... 95  
**emergencies**  
 collecting personal information ..... 242  
 contact persons ..... 242  
 disclosing personal information ..... 115, 284  
**emergency planning** ..... 149  
**emissions**  
 toxic ..... 228

- employees**  
 as confidential sources..... 150  
 as third parties..... 211  
 defined..... 115-116  
 disclosing personal information to..... 274-276  
 disclosure to the Information and  
 Privacy Commissioner..... 43-44, 234, 352-353  
 documenting record transactions..... 316  
 emergency contacts..... 242  
 grievances..... 146  
 identities..... 353  
 personal information disclosure..... 102, 103,  
 115-117, 126, 267, 286-287  
 research information..... 11-12, 193  
**employee directories**..... 289  
**employment**  
 administrative investigations..... 146-147  
 adverse actions..... 44  
 confidential evaluations..... 141-144  
 contracts..... 115-117, 126, 141, 268  
 discretionary benefits..... 115, 117, 268  
 duties..... 115-117, 119, 126  
 educational leave..... 247  
 FOIP training..... 28  
 history..... 7, 126  
 interviews..... 142  
 job classifications..... 115-116, 172, 247, 267, 279  
 job title..... 116, 129  
 job counseling..... 279  
 job responsibilities..... 116, 126, 267  
 offences..... 353  
 pay and benefit services..... 247  
 peer evaluations..... 142  
 pension formula..... 117  
 performance appraisals..... 116, 126, 142, 181  
     distinct from reference checks..... 142  
 personal information..... 7, 116, 126  
 personal service contracts..... 116, 118, 181, 268  
 recruitment..... 247  
 references..... 127, 141, 247, 252, 286  
 selection process..... 141-142, 181  
 staffing requirements..... 181, 247  
 third party evaluations..... 127-128, 132  
**employment history**..... 126  
 employment information, *see employees*,  
 personal information disclosure; **personnel**  
**information**  
**employment insurance**..... 272, 279  
**enactments of Alberta**  
 collecting personal information..... 236  
 disclosing personal information..... 115, 270, 272  
 disclosing third party information..... 111  
 municipal bylaws..... 236  
 routine disclosure..... 32  
**enactments of Canada**  
 collecting personal information..... 236  
 disclosing personal information..... 115, 270, 272  
 disclosing third party information..... 111  
 routine disclosure..... 32  
**endangered forms of life**  
 disclosure harmful to..... 206-207  
**ENMAX Corporation**..... 4  
**enrolment information**  
 post-secondary educational bodies..... 121-122  
 schools..... 121-122, 261  
 Environment, *see Alberta Environment*  
**environment**  
 disclosure to protect fee waiver..... 77, 79  
 personal information..... 130  
 harm to..... 227, 228  
 testing..... 184, 185, 193  
**Environmental Appeals Board**..... 10  
**Environmental Protection and  
 Enhancement Act**..... 111  
**EPCOR Utilities Inc.**..... 4  
**espionage**..... 149  
**estates**  
 administration of..... 246  
**Ethics Commissioner**  
 disclosing personal information to..... 288  
 office..... 2  
 records..... 10-11  
 records excluded from *FOIP Act*..... 10, 11  
**ethnic origin**..... 128, 129  
 personal information..... 6, 128, 129  
**evaluations**  
 confidential..... 141-144  
 keys..... 195  
**examination for discovery**..... 5-6  
 examination of records, *see records*,  
 examination of  
**examination questions**..... 11  
 exceptions, *see FOIP Act*, exceptions  
 exclusions, *see FOIP Act*, exclusions  
**Executive Council**..... 2  
 agenda..... 167, 168  
 appeals..... 169  
 background facts..... 168, 169-170  
 Cabinet confidences..... 96, 166-171  
 confidential information..... 166-171  
 decisions..... 167, 169-170  
 defined..... 166  
 members, *see ministers*  
 minutes..... 168  
 non-arm's length transactions..... 17  
 office..... 2



executors .....	36
existence of records .....	89-90
failure to locate .....	89-90
harm to health or safety .....	92, 139
harm to law enforcement .....	92, 158-159
personal information .....	92, 135
experts	
disclosing personal information to .....	138, 285
<i>Extension of Time Limit</i> ( <i>Model Letter D</i> ) .....	67, Appendix 3
external publications .....	312

## F

<b>factual information</b>	
not advice .....	179-180
not cabinet confidence .....	169-170
personal information .....	254
<b>fair information practices</b> .....	1, 234-235
<b>fair trials</b> .....	153
<b>fairness</b> .....	78-79, 132, 359, 364
<i>Family Law Act</i> .....	38
<b>family relationships</b> .....	132, 290-292
<b>family status</b> .....	6
<b>family violence</b> .....	137
<b>fauna</b>	
conserving .....	206
<b>Federal Bureau of Investigation</b> .....	284
federal government, <i>see</i> <b>Government of Canada</b>	
federation boards, <i>see</i> <b>library boards</b>	
<i>Fee Estimate (Model Letter E)</i> .....	75, Appendix 3
<b>fees</b>	
assessing .....	72-81
collecting .....	25
continuing FOIP requests .....	74
deposits .....	76
estimates .....	25, 75-76
examination of records .....	74
FOIP requests .....	25
GST .....	73
<i>Health Information Act</i> requests .....	56-57
initial fees .....	74
investigations .....	350, 362
local public bodies .....	73
Orders .....	350
payments .....	76-77
personal information requests .....	74-75
reducing .....	52, 77
refunds .....	76
routine disclosure .....	32
schedule .....	74
waivers .....	73, 77-81
<b>Finance and Enterprise</b> <i>see</i> <b>Alberta Finance and Enterprise</b>	

<i>Financial Administration Act</i> .....	16
<b>financial audits</b> .....	280
<b>financial gain</b> .....	108
<b>financial hardship</b> .....	78
<b>financial history</b>	
personal information .....	7, 127
<b>financial information</b> .....	103, 116, 117, 118, 119, 127, 189-192, 252
fee waiver .....	78
public bodies .....	188-192
<b>financial loss</b> .....	108, 188, 191-192
<b>fines</b>	
collection of personal information .....	244
disclosure to collect .....	277-278
offences under the <i>FOIP Act</i> .....	44, 450-46, 94, 235, 335
<b>fingerprints</b> .....	7
<b>fire commissioners</b> .....	282
<b>fire inspections</b> .....	157
<b>firearms</b>	
permits .....	154
technical information .....	154-155
<b>First Nations police services</b> .....	5, 282
<b>fitness requirements</b> .....	124
<b>flora</b>	
conserving .....	206
<b>FOIP Act</b>	
adjudicator process .....	365-366
administration .....	23
advice .....	350, 352
amending .....	29
annual report .....	30, 351
burden of proof .....	360-361
coming in to force dates .....	2, 3, 4
contracts and contractors .....	8
education of the public .....	350
exceptions .....	1, 95-209
advice from officials .....	97, 177-187
audit by Chief Internal Auditor .....	96, 186
Cabinet and Treasury Board	
confidences .....	96, 166-171
confidential evaluations .....	97, 141-144
exposure to civil liability .....	156
harm to business interests .....	101-112, 302
harm to economic and other	
interests of public bodies .....	97, 188-194
harm to historic resources .....	97, 206
harm to individual or public safety .....	97, 137-140
harm to intergovernmental relations .....	97, 161-165
harm to law enforcement .....	97, 145-155, 284-285

- harm to personal privacy ..... 113-136
- individual under supervision of
  - correctional authority..... 156
- interpretation ..... 96-97
- local public body confidences ..... 97, 172-176
- notices.....Appendix 3
- offence under Act of Canada..... 96, 125, 157
- privileged information ..... 97, 196-205, 302
  - third parties..... 96, 197-201, 202-203
- published information..... 207-209
- relevant factors ..... 92
- steps in applying..... 99-100
- exclusions ..... 1, 4, 8-18, 91
  - disclosure..... 20
  - notices.....Appendix 3
- exercise of rights by other persons ..... 36-39
- monitoring ..... 351-352
- offences and penalties..... 44-46, 94, 235, 339, 353
  - destruction of records ..... 316
- policies and procedures ..... 24, 25
- province-wide administration ..... 29-30
- public education..... 350
- purposes..... 1-2, 98, 350
- relationship to other Acts..... 20-21, 25
  - archival records ..... 302-303
- responsibilities under ..... 28-296
- scope ..... 2
- time extensions
  - third parties..... 215-217
- training..... 24, 30
- FOIP Bulletins**
  - No. 1: *Fee Estimates*..... 76
  - No. 2: *Fee Waivers* ..... 81
  - No. 3: *Access to Manuals and Guidelines* ..... 43
  - No. 4: *Disclosure of Personal Information – “Not Contrary to the Public Interest”* .. 123, 268
  - No. 5: *Fund-Raising* ..... 243, 264, 293
  - No. 6: *Records of Elected and Appointed Officials of Local Public Bodies* ..... 15
  - No. 7: *Law Enforcement*..... 125, 145, 237, 284
  - No. 8: *Common or Integrated Programs or Services*..... 277, 294
  - No. 9: *Burden of Proof*..... 361
  - No. 10: *Third Party Notice* ....40, 65, 111, 211, 222
  - No. 11: *Paramountcy*..... 21, 303
  - No. 13: *Business Contact Information*..... 290
  - No. 15: *Disclosure of Personal Information to Unions: Before a First Agreement* ..... 272
  - No. 16: *Personal Information of Deceased Persons* ..... 120, 292
- FOIP contacts, *see* **programs and services**,
- FOIP contacts
- FOIP Coordinator**
  - business contact information ..... 29
  - closure of office..... 68
  - collection of personal information..... 239-240
  - consultations
    - Cabinet and Treasury Board confidences.... 167
    - intergovernmental relations..... 161
  - copies of requests and records ..... 92
  - creating new records..... 83-84
  - delegation instruments..... 27-29
  - duty to assist ..... 24, 50-53, 83-84
  - FOIP requests ..... 24-25, 60-61, 72, 92-93
  - information dissemination ..... 33-35
  - privacy audits..... 25, 251
  - privacy impact assessments..... 237, 330
  - privacy protection..... 235
  - records management..... 26-27
  - relationship with applicants..... 59
  - responsibilities..... 24-25, 68
  - review of records ..... 71-72, 82-83
  - routine disclosure..... 33-35
  - severing information..... 25
- FOIP Office, *see* FOIP Coordinator**
- FOIP (Ministerial) Regulation**
  - public bodies designated by..... 177, 182
- FOIP Regulation**
  - amending ..... 29
  - audits ..... 279-280
  - consent for use of personal information ..... 261-262
  - consent to disclosing personal information 114, 269
  - fee schedule ..... 74
  - harm to applicant's health and safety ..... 138, 285
  - in camera* meetings..... 173-174
  - public bodies..... 25
    - agenda or minutes..... 182
  - relationship of *FOIP Act* to other Acts..... 20-21
  - research agreements..... 299, 303
  - using personal information ..... 261-262
- FOIP requests**
  - abandoning ..... 81
  - access..... 90, 95
  - Access and Privacy role..... 63
  - acknowledging..... 53-54
  - adequacy of search ..... 50-51, 52-53, 69-70, 314-316, 360
  - as last resort ..... 31
  - charts .....Appendix 4
  - clarifying ..... 50-51, 52, 59-60
  - communications strategies..... 26
  - completion ..... 92-94
  - concurrent..... 66-67
  - consultations ..... 62-63, 63-64, 71
  - third parties..... 211-224



continuing, *see* **continuing FOIP requests**  
 copying records ..... 68, 85  
 deemed refusal ..... 64  
 disregarding ..... 57-59, 354  
     time limits ..... 59  
 documenting ..... 60-61, 88, 357, Appendix 5  
 dual processes ..... 51  
 duty to assist ..... 50-51, 83-84  
 evading ..... 45  
 exercising discretion ..... 97-98, 100  
     reconsidering ..... 98  
 fees, *see* **fees**  
 forms ..... 49, Appendix 5  
 frivolous or vexatious ..... 57, 58-59  
**Health Information Act**  
     notices ..... Appendix 3  
*in camera* meetings ..... 173-175  
 initial fees ..... 74  
 language ..... 50  
 legal advice ..... 82  
 legal case records ..... 5-6  
 line-by-line review ..... 82, 86, 100,  
     Appendix 5  
 multiple ..... 66-67  
 narrowing ..... 51-51, 60, 75-76  
 nature of ..... 49, 51  
 notices ..... 63, 67, 72, 81, 211-224, Appendix 3  
 oral requests ..... 49  
 partial disclosure ..... 88, 222  
 personal information ..... 267  
 preliminary assessment ..... 71-72  
 preliminary examination of records ..... 99  
 processing ..... 24-25, 68-92  
 reason for request ..... 51  
 receiving ..... 46-64  
 records excluded from *FOIP Act* ..... 91  
     refusal of access ..... 91  
 records issues ..... 314-316  
 records retention ..... 94, 324  
 refusal of access ..... 86, 88, 89  
 refusal to confirm or deny  
     existence of records ..... 89, 92, 135, 139, 158-159  
 repetitious ..... 57-58  
 responding to ..... 53-54, 68, 87-88, 88-92, 100,  
     350, 357  
     nature of response ..... 53-54  
     notices ..... Appendix 3  
 responsive information ..... 84-85  
 review for routine disclosure ..... 34  
 reviewer's recommendations ..... 82-83  
 routine disclosure ..... 31-32  
 scope ..... 51-52, 60

severing ..... 85-88, 100  
     documenting ..... 53, 96  
     non-responsive information ..... 85  
 statistics ..... 30  
 systematic ..... 57-58  
 time extensions ..... 215-217, 350  
 time limits ..... 64-68, 72, 92-93, 100-101, 215-216,  
     Appendix 4  
 time lines ..... Appendix 4  
 tracking ..... 24, 60, 68, 92, 93  
 transfers ..... 61-63, 71-72  
     notices ..... Appendix 3

**forms**

collection of personal information ..... 236, 249,  
     321-322  
 electronic ..... 335  
 FOIP requests ..... 49  
 review ..... 333-335

foundations, *see* **housing management bodies**

*Freedom of Information and Protection  
 of Privacy Act*, *see* **FOIP Act**

Freedom of Information and Protection of Privacy  
 Regulation, *see* **FOIP Regulation**

**frivolous or vexatious FOIP requests** ..... 57, 58-59

**function creep** ..... 253, 295

**fund-raising**, *see also* **Charitable Fund-raising Act**

    alumni records ..... 263-264, 293, 307

    collecting personal information ..... 243

    disclosing personal information ..... 293

**G**

**gangs** ..... 151

**genealogical research** ..... 120

**general faculties councils** ..... 15, 173

gender, *see* **sex**

**genetic information** ..... 6

**Glenbow-Alberta Institute**

    archives ..... 282

**good faith** ..... 43-44, 234

goods and services tax, *see* **GST**

**good will** ..... 108, 192

**governing bodies**

    advice and deliberations ..... 177

    agenda or minutes ..... 182

    appointees ..... 116

    correspondence of members ..... 15

    designation of head of public body ..... 23-24

    meetings ..... 173

    membership information ..... 207

    personal records ..... 15-16

    post-secondary educational bodies ..... 15, 173

    roles and responsibilities ..... 24-24

**government institution** ..... 5  
**Government of Alberta** ..... 2  
     as sovereign power ..... 162, 189  
     economic interests ..... 188-194  
     intergovernmental relations ..... 161-165  
     investment strategies ..... 189  
     negotiations ..... 162, 164, 181, 191-192  
     non-arm's length transactions ..... 111  
     personnel management ..... 247-248, 286-287  
**Government of Alberta Call Centre** ..... 49  
**Government of Alberta Policy for the  
     Transmission of Personal Information  
     via Electronic Mail and Facsimile** ..... 313  
**Government of Alberta Technology  
     Security Policy** ..... 313  
**Government of Canada**  
     intergovernmental relations ..... 161-165  
**Government Organization Act** ..... 253  
**Government Security Policy for Disk Wiping  
     Surplus Computers** ..... 259  
**graduations**  
     lists of graduates ..... 121  
**grants** ..... 119-120  
     eligibility for ..... 279  
**grievances** ..... 132, 146  
**GST** ..... 73  
**guardians or trustees** ..... 36, 134, 246  
     authentication of ..... 36  
     exercising rights of individuals ..... 36  
**guardians of minors** ..... 37-39  
     authentication of ..... 38  
     exercising rights of individuals ..... 37-39  
**Guide to Developing Personal Information  
     Sharing Agreements** ..... 272, 327, 343  
**Guide to Developing Privacy Statements for  
     Government of Alberta Web Sites** ..... 334  
**Guide to Identifying Personal  
     Information Banks** ..... 41, 304, 309  
 guidelines, *see* **polices and procedures; FOIP Act,**  
     **polices and procedures**

## H

**harassment** ..... 137  
**hard drives** ..... 307, 311  
**harm**  
     atmosphere ..... 228  
     audit procedures ..... 195  
     business interests ..... 101-112  
     determining ..... 87, 99, 106-107, 137  
     economic interests of public bodies ..... 188-189  
     environment ..... 225, 228  
     exposure to ..... 121, 132  
     financial gain ..... 108

    financial loss ..... 108, 188, 191-192  
     health or safety ..... 137-140, 225, 228  
     historic resources ..... 206  
     individual under supervision of  
         correctional authority ..... 156-157  
     intergovernmental relations ..... 161-163  
     law enforcement ..... 145, 147-148, 150, 152  
     monetary value ..... 108  
     privacy ..... 113-136  
     probability of ..... 99, 107  
     public interest ..... 120, 121, 225, 229-230  
     specifying ..... 99  
**harms tests** .... 99, 106-107, 137, 145, 148, 149, 150,  
     152, 155, 156, 162, 188-189, 193  
**heads of public bodies**  
     advice and deliberations ..... 177  
     advice from Information and Privacy  
         Commissioner ..... 350, 352  
     disclosing personal information to ..... 275  
     disclosing personal information about  
         deceased individuals ..... 120, 291  
     disclosure harmful to  
         intergovernmental relations ..... 161  
     disclosure in public interest ..... 225  
         not contrary to ..... 120-121  
     discretion (health and safety exception) ..... 292  
     discretionary exceptions reconsidering ..... 98  
     disregarding FOIP requests ..... 354  
     duties, directory of personal  
         information banks ..... 41-42, 235, 27  
     duty to assist ..... 51  
     exercising discretion ..... 97-98, 292  
     Information and Privacy Commissioner... 351, 365  
     requiring Information and Privacy  
         Commissioner to examine records ..... 354, 359  
     responsibilities ..... 23-24, 350  
**health** ..... 7  
     audits ..... 105  
     disclosure endangering ..... 115, 121  
     disclosure harmful to ..... 137-140, 268  
         refusal to confirm or deny existence  
             of records ..... 92  
     harm to ..... 225, 228  
     imminent danger to ..... 292  
     personal information ..... 55-57, 124, 130, 137-140  
 Health and Wellness, *see*  
     **Alberta Health and Wellness**  
**health care**  
     personal information ..... 6, 18, 55-57, 124, 130,  
         138, 272  
         expert consultations ..... 138, 139, 284, 286  
     research ..... 193  
**health care bodies** ..... 3

<b>Health Information Act</b> .....	10, 55-57, 75, 124, 138, 225, 241, 283, 288, 328-329, 331-332, 340, 344
access requests	
notices .....	Appendix 3
section 1(1)(k) .....	18
section 8(1) .....	56
<b>Health Information Act Guidelines and Practices Manual</b> .....	57, 322, 336, 344
<b>health services program</b> .....	238
<b>hearing-impaired persons</b>	
FOIP requests .....	49
<b>historic resources</b>	
disclosure harmful to .....	206
impact assessments .....	206
historic sites .....	206
historical research, <i>see</i> <b>research</b> , historical	
<b>Historical Resources Act</b> .....	206
<b>holidays</b> .....	68
<b>honours</b>	
receipt of .....	122
suitability for .....	242-243, 343
<b>hospital boards</b> .....	3
<b>hospitals</b>	
prisoner in .....	156
<b>Hospitals Act</b> .....	3
<b>housing</b>	
low-income .....	141, 245
continuing eligibility for .....	246
student .....	141
<b>housing management bodies</b> .....	4, 14
audits .....	280
personal information .....	263
human resources, <i>see</i> <b>employment; personnel management</b>	
<b>Human Resources and Social Development Canada</b> .....	272
<b>Human Resources Guide for Local Public Bodies</b> .....	287
<b>human rights panels</b> .....	153

## I

<b>identifiers</b>	
removal .....	296
<b>identity</b>	
applicants .....	35, 69, 214, 219
confirming .....	322
confidential sources .....	150-151
employees .....	43, 103, 353
police informers .....	150-151, 199
proof of .....	35, 37, 38, 89
third parties .....	214-215, 217
<b>images</b> .....	6

<b>IMAGIS account</b> .....	77
<b>implementation</b>	
public body plans .....	181
<b>improvement districts</b> .....	3
<b>in camera meetings</b>	
disclosure .....	264
local public bodies .....	173-175
minutes .....	175
municipalities .....	173
personal notes .....	175
<b>income assistance</b> .....	119-120, 125, 245, 252
Alberta Seniors Benefit .....	272
<b>incompetent individuals</b> .....	36-37, 263, 357
<b>Indian Act (Canada)</b> .....	162
Indian people, <i>see</i> <b>aboriginal people</b>	
indirect collection, <i>see</i> <b>personal information</b> , indirect collection; <b>collection of personal information</b> , indirect	
<b>industrial sabotage</b> .....	149, 152
<b>information, <i>see also</i> personal information</b>	
5 years old	
Cabinet decisions .....	101, 169, 170
10 years old	
prosecutorial discretion .....	153
15 years old	
administration and management of a	
public body .....	182
advice from officials .....	101, 183
audit by Chief Internal Auditor .....	101, 186
Executive Council or	
Treasury Board .....	101, 168
intergovernmental relations .....	101, 164
local public body confidences .....	101, 175
25 years old	
disclosure by archives .....	301
50 years old	
businesses .....	100, 111
available for purchase .....	207
correctional records .....	155-156
clarifying .....	53-54
disclosure in public interest .....	225-232
disclosure policies .....	98
failure to publish .....	209
individually identifiable .....	6-7
law enforcement records .....	124-125, 145-160
leaks .....	169
local public body confidences .....	172-176
not records .....	226
outside the FOIP process .....	60
published .....	102, 207-209, 289-290
fund-raising .....	243
readily available to the public .....	207
revealing classes of .....	99

- advice from officials..... 177-187  
 audit by Chief Internal Auditor ..... 19, 186  
 Cabinet confidences ..... 166-171  
 confidential sources..... 150  
 correctional records ..... 155-156  
 criminal intelligence ..... 151  
 exercise of prosecutorial discretion ..... 152  
 local public body confidences ..... 172-176  
 records seized ..... 153  
 routine disclosure..... 32  
 technical information..... 154  
 third party legal  
     business ..... 101-112  
     privileged..... 196-201, 202-203  
**Information and Privacy Commissioner**..... 30,  
     349-367  
     adjudicator process ..... 365-366  
     adjudicators..... 365, 366  
     advice..... 350, 352  
         defined..... 166, 179  
     advice to heads of public bodies..... 350, 352  
     annual report..... 30, 350, 351  
     appeals  
         fees ..... 81  
     appointment ..... 349  
     approval of research purposes ..... 297  
     as public body ..... 351, 365  
     audits ..... 25, 351, 364  
     burden of proof..... 74, 360-361  
     comments  
         proposed legislation..... 350, 351  
         proposed programs ..... 350, 351  
     complaints, *see* **complaints**  
     conflict of interest..... 365  
     consultation..... 21  
     contempt of court..... 353, 359  
     data matching..... 344, 346-347, 352  
     decisions ..... 96  
     delegation by ..... 355, 366  
     disclosure of information by ..... 354-355  
     disclosure of third party information ..... 102, 221  
     disclosure to ..... 43-44, 288, 352-353  
     disclosure to Minister of Justice and  
         Attorney General..... 355  
     discretionary exceptions  
         orders ..... 98  
     disregarding FOIP requests ..... 57-59, 354  
     duty to assist applicants  
         comments ..... 50-51  
     education of the public ..... 350  
     evidence in proceedings..... 354  
     examination of records ..... 353-354, 359  
     excluded records ..... 10, 89  
     forms..... Appendix 5  
     frivolous or vexatious requests ..... 58-59  
     *in camera* hearings ..... 359  
     indirect collection of personal information..... 241,  
         335, 350  
     inquiries ..... 358-360  
         request for authorization to disregard  
             request during ..... 58  
         refusal to conduct ..... 359-360  
         review of refusal ..... 360  
     Investigation Reports..... 363  
     investigations..... 25, 30, 234, 350, 362-364  
         disclosure by employees..... 43, 234, 353  
         duty to assist..... 350, 362  
         failure to disclose in public interest..... 231, 351  
         fees ..... 350, 362  
         information other than personal ..... 350  
         personal information correction ..... 350, 362  
         powers ..... 350-351, 353-354, 362  
         record destruction ..... 351  
         records management..... 306  
         time extensions..... 350, 362  
     judicial review ..... 355, 360, 364-365  
     jurisdiction..... 21, 360, 364  
     labour relations ..... 108-109  
     mediation ..... 358  
     monitoring *FOIP Act*..... 351-352  
     notices ..... 39-40  
         substitutional service ..... 39-40, 217  
     notification of disclosure in  
         public interest..... 230-231  
     obstruction ..... 45  
     offences ..... 45, 353, 354, 362  
         laying charges..... 355  
     office..... 2  
     Orders ..... 30, 350, 361-362  
         administrative matters ..... 30  
         authorizations to disregard requests, not ..... 58  
         availability..... 351, 362  
         compliance ..... 362  
         copies sent to parties..... 362  
         discretionary exceptions ..... 98, 361  
         fees ..... 350  
         judicial review ..... 355, 364-365  
         mandatory exceptions..... 361  
         offences ..... 45, 362  
         personal information ..... 30, 350  
         time extensions..... 350  
         time limits..... 362  
         types ..... 361  
     parliamentary privilege..... 199  
     personal information requests..... 55  
         disregarding..... 59



- portfolio officers ..... 358, 363
- powers ..... 350-351, 353-354
  - delegation ..... 355, 366
  - inquiries ..... 350-351, 353-354
  - investigations ..... 350-351, 353-354, 362
  - initiating ..... 363
  - limits ..... 350, 362
- practice notes, *see* **IPC FOIP Practice Notes**
- privacy audits ..... 351, 364
- privacy impact assessments ..... 237, 328, 330-331, 336
- privacy protection ..... 351-352
- privileged information ..... 353
  - Solicitor-Client Adjudication Protocol* ..... 197, 353
- producing records for ..... 353-354
  - time limits ..... 353
- protection from liability ..... 355
- public education role ..... 350
- public interest
  - determination ..... 229-230
  - fee waivers ..... 77, 79-81
- publications, *see* **IPC FOIP Practice Notes**
- records excluded from *FOIP Act* ..... 20, 91
- record linkage
  - comments ..... 350
- records management ..... 306-307
- refusal to confirm or deny existence
  - of records ..... 89
- removal from office ..... 349
- Request for Review Form* ..... Appendix 5
- requesting a review ..... 88
- research ..... 350, 352
- responsibilities ..... 30, 349-356
  - records management ..... 306-307
- retention of records reviewed ..... 354
- review process ..... 357-358
- reviews, *see* **reviews**
- security plan ..... 336
- severing information ..... 357, 358
- Solicitor-Client Adjudication Protocol* .... 197, 353
- statements provided to ..... 354-355
- term of office ..... 349
- third party consultations ..... 213
- time extensions ..... 64-66, 350, 362
  - third party notification ..... 215
- Information Assets in the Government of Alberta:**
  - A Management Framework* ..... 306
- information dissemination** ..... 33-35
- information management** ..... 305-317
  - policy and procedures ..... 308-314
  - principles ..... 306-307
- Information Management Planning** ..... 306
- Information Security Classification** ..... 306
- information technology and systems**
  - active dissemination ..... 34
  - planning ..... 308-309, 313-314, 327-328, 335
  - policies and procedures ..... 308-314
  - privacy protection ..... 314, 319-348, 351
  - records management ..... 26, 83-84, 313-314
  - risk classification ..... 337
  - security ..... 259, 336-340
  - threat and risk assessments ..... 337, 340-342
- Information Technology Security Policy** ... 336, 337
- Infrastructure, *see* **Alberta Infrastructure**
- infrastructure**
  - provincial ..... 164, 189
  - security of ..... 149
- inheritable characteristics** ..... 7
- inheritance rights** ..... 131
- inmates**
  - hospitals ..... 156
  - legal representatives ..... 292
- inquiries, *see* **Information and Privacy Commissioner, inquiries**
- inspections**
  - fire ..... 157
  - liquor licensing ..... 157
  - practices ..... 189
  - public health ..... 157
  - reports ..... 104, 157-158
  - routine
    - law enforcement ..... 157
    - routine disclosure ..... 33
  - vehicle safety ..... 157
- integrated programs or services, *see* **programs and services, integrated**
- insurance policies** ..... 183
- intelligence tests** ..... 11, 195
- intergovernmental relations**
  - negotiations ..... 161-165
  - records
    - 15 years old ..... 164
  - refusing to disclose information ..... 161-165
- International and Intergovernmental Relations, *see* **Alberta International and Intergovernmental Relations**
- international bodies**
  - intergovernmental relations ..... 161, 162
- International Standards Organization Records Management Standard (ISO 15489)** ..... 305
- Internet, *see also* electronic records**
  - active dissemination ..... 33
  - collecting personal information through ..... 334
  - disclosing personal information on ..... 265, 289, 290
  - publicly available information ..... 207, 208, 243

notices on..... 321  
 routine access..... 33  
*Internet and E-mail Use Policy*..... 336  
**Interpol**..... 284  
*Interpretation Act*..... 64, 68  
**interviews**..... 142  
     collection of personal information..... 236, 246  
     notes  
         retention..... 252  
     questions..... 195  
 Inuit people, *see* **aboriginal people**  
**investigations**  
     administrative..... 124, 146-147  
         authority for..... 146  
     bylaw..... 145  
     collection of personal information..... 243-244  
     complaints as part of..... 125, 145, 234  
     disclosure of personal information for..... 124, 282-284  
     evidence..... 363  
     Information and Privacy Commissioner,  
         *see* **Information and Privacy Commissioner, investigations**  
     investigative techniques..... 150  
     law enforcement..... 124, 145-147  
         disclosure form..... Appendix 5  
         interference with..... 152  
         ongoing..... 126  
     police..... 124, 145, 146  
         completed..... 158  
     records, exemption..... 10  
     security..... 124, 145, 146, 339  
     *Water Act*..... 147  
     workplace..... 126  
**investment strategies**..... 103, 191  
     public bodies..... 188  
**IPC FOIP Practice Notes**  
     1. *Applying "Harms" Tests*..... 99, 148  
     2. *Informing the Applicant of Grounds for Refusal*..... 88, 357  
     3. *Complaints About Public Bodies – "Reviews" Versus "Investigations"*..... 364  
     4. *Section 4 – Exclusions from the Act*..... 18, 353  
     5. *Preparing Records and Submissions for Inquiries*..... 357  
     7. *Privacy Complaints – Investigations and Inquiries*..... 363  
     9. *Authorization to Disregard Request Under Section 55*..... 59  
**Irrigation Board**..... 4  
*Irrigation Districts Act*..... 4

**J**

jobs, *see* **employment**  
**job title**..... 116, 129  
**judges**  
     records..... 9  
**judicial administration records**..... 9  
**judicial review**..... 355, 360, 364-365  
**judicial or quasi-judicial capacity**..... 9  
**judicial tribunals**  
     criteria for determining..... 9  
     disclosure of personal information to..... 285-286  
     draft decisions..... 9  
     personal note..... 9  
     rules..... 5  
 Justice and Attorney General, *see* **Alberta Justice and Attorney General**  
**justices of the peace**  
     records..... 9

**L**

**labour relations**  
     disputes..... 108-109  
     *in camera* meetings..... 174  
     information..... 103, 108-109  
         implicitly reveal..... 108  
     mediation..... 109  
     negotiations..... 181  
     officers..... 109  
     third parties..... 108  
 Labour Relations Board, *see* **Alberta Labour Relations Board**  
**labour unions**  
     archival records..... 12  
     associations..... 6  
     collective agreements..... 103  
     disclosing personal information to..... 281-282  
**land claims**..... 132, 162, 248  
**Land Titles Offices**..... 13-14  
**landfills**  
     testing..... 184  
**landlord**  
     character references..... 127  
**law enforcement**  
     agencies..... 282-284  
     collection of personal information..... 237, 243-244  
         must meet definition of..... 237  
     complaints..... 125, 145, 148  
     confidential sources..... 150-151, 199-200  
     criminal intelligence..... 145, 151  
     disclosure harmful to..... 145-160, 268  
     disclosure of personal information for..... 282-284  
     forms..... Appendix 5



- examination of information by Information and Privacy Commissioner ..... 355
- harm..... 145, 147-148, 150, 152,
- in camera* meetings..... 174
- inspections..... 157
- investigations..... 124-125, 145-147
  - completed..... 158
  - interference with..... 152
- investigative techniques..... 150
- penalties or sanctions..... 145-147, 243-244
- privileged information..... 199-200
- privacy impact statements ..... 237
- proceedings..... 147
- records
  - confiscated records..... 153-154
  - correctional record..... 155
  - custody or control..... 145-147
  - disclosure an offence under Act
    - of Canada..... 157
    - personal information..... 124-125
    - severing information..... 87
  - records of disclosure..... 284
- refusal to confirm or deny existence
  - of records ..... 92, 158
- reports and publications..... 154, 155, 157-158
- routine inspections..... 157
- statistical information..... 158
- unsolved investigations
  - interference with..... 152
  - video surveillance..... 150, 236, 237, 244
- Law Enforcement Disclosure Form**.....Appendix 5
- law reports**..... 290
- lawsuits**..... 130, 132, 156
- leaks of information**..... 169
- leases**..... 108
- legal agents**..... 201, 202
- legal interpretation**..... 50
- legal matters**
  - advice..... 197, 202
    - compliance with subpoena, warrant
      - or order ..... 274
  - applicant's rights ..... 131-132
  - civil legal cases... 5-6, 131-132, 148, 153, 156, 277
  - collection of personal information..... 245
  - correspondence ..... 197-198, 202
  - criminal legal cases..... 5-6
  - disclosure of personal information ..... 277
  - fair trial ..... 153
  - FOIP advice..... 87
  - impartial adjudication..... 153
  - in camera* meetings..... 174
  - legal actions..... 131-132, 148, 153, 156
  - legal instruments..... 172
  - legal opinions**..... 197-198, 202
  - legal privilege**..... 86, 196-205
    - severing ..... 86
  - legal proceedings**..... 5-6, 153
    - access to records..... 5-6, 12
    - collection of personal information..... 245
    - disclosure of personal information .. 131-132, 277, 285-286
    - effect on court powers ..... 6
    - law enforcement ..... 147
  - legal representatives**
    - inmates..... 292
  - legislation**
    - consultation about..... 19, 351
    - drafts..... 166, 172, 182
      - Executive Council ..... 166, 182
      - Information and Privacy Commissioner comments ..... 350, 351
      - local public bodies..... 172
    - information readily available to public..... 207
    - interpretation ..... 185
  - Legislative Assembly**..... 18, 349
  - Legislative Assembly Act**..... 272, 275
  - Legislative Assembly Office**..... 2, 16
  - Letter to Speaker of the Legislative Assembly Regarding Parliamentary Privilege (Model Letter K)**..... 199, Appendix 3
  - letters**..... 6
    - elected officials..... 14
    - governing bodies ..... 15-16
    - ministers, MLAs..... 16-17
    - officers of the Legislature..... 10
  - Letters to Experts Under Section 18(2)**
    - Initial Letter (Model Letter V)*.....Appendix 3
    - Transmission of Records (Model Letter W)*.....Appendix 3
  - liabilities**
    - financial
      - public bodies ..... 188, 191-192
  - liability**
    - civil
      - discretionary exceptions..... 156
      - protection from ..... 44, 355
      - public bodies..... 95
  - libraries**
    - active dissemination ..... 33, 207, 208
    - head ..... 24
    - information dissemination..... 33, 207
    - membership ..... 279
    - published works collected by ..... 12
    - school-housed ..... 277
  - Libraries Act**..... 4
  - library boards**..... 4

library system board, *see* **library boards**

**licences**

- drivers ..... 13
- personal information disclosure ..... 118-119, 268
- suspension or revocation ..... 119
- trade secrets ..... 102, 190

**licensing**

- practices ..... 189

**Lieutenant Governor in Council**

- designation powers ..... 349
- draft judicial or quasi-judicial decisions ..... 9-10
- power of appointment ..... 34

**literacy**

- FOIP requests ..... 49

**litigation privilege** ..... 198-199

**local government bodies** ..... 3-4

- confidential information ..... 172-176
- exclusions ..... 4-5
- intergovernmental relations ..... 161-165

local public bodies, *see also* **educational bodies, health care bodies, local government bodies, post-secondary educational bodies, public bodies**

**local public bodies** ..... 2

- bylaws ..... 6, 172
- databases ..... 33
- directories of records ..... 41-42
- elected officials ..... 14-15
- elections ..... 15
- fee structures ..... 72
- heads ..... 23-24
- in camera* meetings ..... 172-176
  - authority for ..... 173-175
- meetings ..... 173
- non-arm's length transactions ..... 111
- personal information disposition ..... 259
- personal information banks .. 41-42, 235, 261, 272, 307
- personnel management ..... 286
- records management ..... 6, 306
  - FOIP requests ..... 94
- security ..... 146
- security planning ..... 149
- transitory records ..... 239, 311

long-term care facilities, *see* **nursing homes**

## M

**maintenance enforcement**

- collection of personal information ..... 246
- disclosure of personal information .... 246-247, 287

**Maintenance Enforcement Act** ..... 246-247, 272-273, 287, 303

management bodies, *see* **housing management bodies**

**Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators** ..... 8, 101, 104, 235, 260, 280, 314

**Managing Electronic Mail in the Government of Alberta** ..... 306, 313, 336

**mandatory exceptions** ..... 96-97

- Cabinet and Treasury Board
  - confidences ..... 166-171
- Chief Internal Auditor
  - audit information ..... 19, 186
- creating new records ..... 35
- harm to business interests ..... 101-112, 302
  - steps in applying ..... 111-112
- harm to personal privacy ..... 113-136
- notices ..... Appendix 3
- offence under Act of Canada ..... 157
- privileged information
  - third parties ..... 202-203
- public interest ..... 96
- tax information ..... 109-110,

**manuals and guidelines**

- accessing ..... 42-43, 185, 207-208
- available for purchase ..... 42, 207

**mapping data**

- proprietary interest ..... 191

**maps** ..... 6, 207

**marital status** ..... 6

**marketplace**

- regulating ..... 189

**media**

- specialized ..... 86

**mediation**

- Information and Privacy Commissioner ..... 358
- labour relations ..... 108-109

**mediator** ..... 108, 109

**medical records** ..... 200

**medical information** ..... 124, 138, 238

**medical interpretation** ..... 53, 138

**meetings**

- local public bodies ..... 173

**Members of Parliament** ..... 280

**Members of the Legislative Assembly (MLAs)**

- correspondence ..... 16-17
- disclosing personal information to ..... 280-281
- offices ..... 4, 16
- records excluded from *FOIP Act* ..... 4, 16

**memory aids** ..... 15

**mental disabilities** ..... 6

mental health, *see* **health**

**metadata** ..... 313

Metis people, *see* **aboriginal people**  
**Metis settlements** ..... 4  
*Metis Settlements Act* ..... 4  
**Metis Settlements General Council** ..... 4  
**Metropolitan Police** ..... 284  
 Minister of Service Alberta, *see*  
     **Minister responsible for the FOIP Act**  
**Minister of Justice and Attorney General** .... 201,  
     285, 286  
     as legal agent ..... 201-202  
     correspondence ..... 196, 201-202  
     disclosure to by Commissioner ..... 355  
     prosecutions ..... 152-153  
**Minister responsible for the FOIP Act**  
     adjudicator's expenses ..... 366  
     annual report ..... 29  
     copies of orders ..... 351, 362  
     Directory of Public Bodies ..... 29  
     FOIP Coordinator ..... 24  
     intergovernmental relations ..... 163  
     record of purpose notification ..... 303-304  
     responsibilities ..... 29  
**ministers**  
     advice and recommendations ..... 177, 178-180  
     advice to ..... 177-187  
     briefing books or binders ..... 18-19  
     constituency records ..... 16  
     consultations or deliberations ..... 177, 180-181  
     correspondence ..... 16-17, 168  
     designating heads ..... 23  
     disclosing personal information to ..... 274-276  
     non-arm's length transactions ..... 17  
     offices ..... 2  
     orders, drafts of ..... 182  
     personal records ..... 16  
     records ..... 12  
     statements ..... 169  
**ministries**  
     obligations to Schedule 1 public bodies ..... 25  
**minors**  
     access to records ..... 47  
     exercising rights of ..... 37-39  
**minutes**  
     consultations or deliberations ..... 180  
     Executive Council ..... 167, 168  
     *in camera* meetings ..... 175  
     public bodies ..... 177, 182  
**Model Letters** ..... 39, 72, Appendix 3  
**monetary value**  
     discretionary benefits ..... 117  
     economic interests of public bodies ..... 188, 189,  
         191, 193  
     third party business interests ..... 106, 108

**Motor Vehicle Accident Claims Act** ..... 293  
**Motor Vehicle Services Registry** ..... 13-14  
 Municipal Affairs, *see* **Alberta Municipal Affairs**  
**municipal councillors** ..... 14-15  
**Municipal Government Act** ..... 3-4, 109, 236  
     *in camera* meetings ..... 174  
     part 15.1 ..... 4  
     sections 299-301 ..... 19  
 municipal library boards, *see* **library boards**  
**municipalities** ..... 3  
     bylaws ..... 125, 172  
     closure of office ..... 68  
     head ..... 23-24  
     historic resources ..... 206  
     *in camera* meetings ..... 173  
     police commissions ..... 4  
     policing committees ..... 4  
     tax information ..... 109, 127  
     twinning ..... 162  
**Mutual Legal Assistance Treaty** ..... 271

## N

**names**  
     personal information ..... 6  
     unreasonable invasion of privacy ..... 128, 129  
**national origin**  
     personal information ..... 6  
**national security** ..... 149  
 native people, *see* **aboriginal people**  
**natural gas leaks** ..... 228  
**negotiations**  
     aboriginal people ..... 162  
     contractual ..... 181, 191  
     disclosing information ..... 181  
     economic interests ..... 191-192  
     intergovernmental relations ..... 162, 164  
     positions ..... 106-107  
     public bodies ..... 181, 191  
     third parties ..... 106-107, 191  
**next of kin** ..... 242, 243  
**non-arm's length transactions** ..... 17, 111  
**Northern Alberta Development Council** ..... 17  
**notes** ..... 6  
     handwritten ..... 6  
     interviews ..... 252  
     personal, *see* **personal notes**  
     transitory records ..... 312  
**Notice of Processing Request for Correction**  
     **Under Health Information Act**  
         **(Model Letter S.1)** ..... Appendix 3  
**Notice of Processing Request Under**  
     **Health Information Act (Model Letter A.1)** .... 55,  
         Appendix 3

**Notice to Public Bodies in Receipt of Personal****Information (Model Letter U).....258, Appendix 3****notices**

- applicants..... 219, 221, 222
- collection of personal information..... 248-250, 303-304, 315-317
- exceptions..... 250
- oral..... 249, 334
- continuing FOIP requests .....Appendix 3
- copies..... 249, 335
- correction of personal information ..... 257-258
- data matching..... 347
- delivery method..... 39-40
- disclosure of personal information ..... 115, 230-231, 276
- disclosure to experts .....Appendix 3
- fee estimates ..... 75-76
- FOIP requests ..... 72, 93
  - abandoning ..... 81
  - transfers ..... 63
- Health Information Act*.....Appendix 3
- granting access.....Appendix 3
- parliamentary privilege.....Appendix 3
- public bodies.....Appendix 3
- public interest disclosure ..... 230-231
- reasons for disclosure ..... 221
- refusal to confirm or deny existence
  - of records .....Appendix 3
- representatives ..... 40
- of reviews ..... 360
- service of ..... 39-40, 217
  - substitutional service ..... 39-40, 217
  - electronic form ..... 39-40, 217
- third parties ..... 40, 67, 115, 211-224
  - content ..... 218
  - correction of personal information ..... 257-258
  - written..... 211, 219
  - verbal..... 219
- time extensions ..... 67, 215-217

**Notices to Applicants Regarding Third Party****Notification (Model Letters)**

- Section 30(5) Notice (Model Letter M)..... 219,**  
Appendix 3
- Section 31 Decision (Model Letter O)..... 222,**  
Appendix 3

**Notices to Third Parties (Model Letters)**

- Section 17(2)(b) Disclosure of Personal**  
**Information (Model Letter R).... 115, Appendix 3**
- Section 30 (Model Letter L) .....218, Appendix 3**
- Section 31 Decision (Model Letter N)..... 222,**  
Appendix 3
- Section 32 (Prior to Public Interest**  
**Disclosure) (Model Letter P) ....231, Appendix 3**

**Section 32 (After Public Interest**

**Disclosure) (Model Letter Q)....231, Appendix 3**  
notification, *see* **notices**

**Notification Concerning Request**

**For Correction (Model Letter T) ..... 256, 258,**  
Appendix 3

**Notification During Continuing**

**Request (Model Letter B) .....55, Appendix 3**

**numbers or symbols**

personal information..... 7

**nursing homes ..... 3**

admission to..... 279

**Nursing Homes Act..... 3**

**nursing programs..... 277**

**O**

**Occupational Health & Safety Act..... 107**

OECD, *see* **Organization for Economic**

**Cooperation and Development**

Office of the Chief Electoral Officer, *see* **Chief**  
**Electoral Office**

Office of the Chief Internal Auditor, *see* **Chief**  
**Internal Auditor**

Office of the Corporate Chief Information Officer,  
*see* **Corporate Chief Information Officer**

Office of the Information and Privacy  
Commissioner, *see* **Information and**  
**Privacy Commissioner**

Office of the Public Guardian, *see* **Public Guardian**  
**officers**

public bodies

disclosing personal information to ..... 275

**Officers of the Legislature, *see also* Auditor**

**General, Chief Electoral Officer, Ethics**  
**Commissioner, Information and Privacy**  
**Commissioner, Ombudsman**

administrative files ..... 11

disclosure of personal information to ..... 288

records excluded from *FOIP Act*..... 10

**offices ..... 2**

agenda or minutes..... 177, 182

public bodies

closure ..... 69

**Official and Transitory Records: A Guide**

**for Government of Alberta Employees ... 306, 312**

**oil fields ..... 149**

**Ombudsman ..... 350**

disclosing personal information to ..... 288

office..... 2

records excluded from *FOIP Act*..... 10

**Operator Licensing and Vehicle Control**

**Regulation..... 147**



**opinions**  
     correction of..... 254-255  
     personal information..... 7  
**oral disclosure** ..... 113, 265  
     statement of confidentiality ..... 105  
**oral requests** ..... 49  
**orders**  
     authorizations to disregard requests, not ..... 58  
     disclosing personal information..... 273-274  
**Organization for Economic  
   Cooperation and Development** ..... 234  
     fair information practices..... 234  
**outsourcing** ..... 286-287

**P**

**palaeontological resources**..... 206  
**papers**..... 6  
 paramouncy, *see* **FOIP Act**, relationship to  
     other Acts  
**parents**  
     guardianship status ..... 38  
**parliamentary privilege** ..... 199-200  
     notices..... Appendix 3  
**parole** ..... 154, 155, 156, 245  
**partnerships**..... 211, 233  
**patently unreasonable**..... 239  
**Payment System Corporation**..... 278  
**payments**  
     disclosure to make ..... 277-278  
**Peace Officer Act** ..... 153  
**peace officers** ..... 153-154  
**peer evaluations**..... 142  
**penalties**  
     **FOIP Act**..... 44-46  
**penalties or sanctions**  
     breach of security ..... 339  
     law enforcement ..... 145-147  
**pensions**..... 117  
**permits**  
     firearms..... 154  
     personal information disclosure..... 118-119  
     property ..... 118-119, 268  
     suspension or revocation ..... 119  
**Personal Directives Act**..... 36  
**personal information**  
     access..... 1-2, 55-57, 95  
     accuracy ..... 234, 250-252  
     compliance reviews ..... 319  
     defined..... 251  
     delegation of authority..... 27  
     every reasonable effort to ensure..... 250-252  
     agents..... 36-37

agreements authorizing disclosure  
     contents of ..... 271-272  
 annotation ..... 256-257  
     forms ..... 256-257  
 anonymizing ..... 264  
 awards..... 122-123  
 collection ..... 235-240  
     agreements between public bodies ..... 236  
     audits ..... 335  
     authority ..... 235-239  
     best practices ..... 334-335  
     compliance reviews ..... 319-327  
     collecting fines or debts..... 244  
     contracts and contractors ..... 236  
     correctional authorities or institutions .. 244-245  
     direct..... 234, 320  
     emergencies ..... 242  
     employees ..... 352-353  
     forms ..... 249, 333-335  
     from Internet..... 243  
     from other public bodies..... 241-242  
     fund-raising ..... 243  
     honours or awards ..... 242-243, 343  
     indirect..... 234, 237, 240-248, 335, 345, 350  
     interviews ..... 236, 249  
     investigations..... 243-244, 350, 362-364  
     law enforcement ..... 237, 243-244  
     legal matters ..... 245  
     legal proceedings..... 245  
     limitations on..... 237-239  
     maintenance enforcement..... 246-247  
     means of collecting..... 236  
     methods ..... 239-250, 320-321  
     notices ..... 234, 248-250, 321-322, 333-335  
         exceptions..... 250  
     personnel management ..... 247-248, 353  
     programs and services ..... 237-239  
     provision of legal services ..... 245  
     purposes..... 234, 235-239, 260-261, 294-296  
     registries ..... 13  
     retention..... 234, 323-324  
     review of practices ..... 239  
     unauthorized ..... 259-260, 353  
 compiling ..... 261, 268  
 completeness ..... 251  
 confidential ..... 132-133, 139, 150-151  
 consent to disclosure..... 114-115, 281  
     bargaining agents..... 281  
     exercise by other persons ..... 115  
     MLAs ..... 280-281  
     procedures ..... 269  
 consent to new uses  
     procedures ..... 262

- consistent use ..... 261, 268-269, 294-295  
 constraints on disclosure ..... 264, 276-277, 278,  
     300-302  
     law enforcement ..... 283  
 constraints on use ..... 264, 294-295  
 correction ..... 2, 63, 234, 253-259, 304-305  
     delegation of authority ..... 27  
     duty to assist ..... 50  
     investigations ..... 350-362  
     notices ..... 257-258  
     opinions ..... 254-255, 256  
     refusal ..... 256  
     time limits ..... 250, 258  
 data matching ..... 297-298, 326-327, 329,  
     343-348, 352  
 data sharing ..... 326-327, 329, 343-348  
 deceased individuals ..... 36, 120, 268,  
     290-292, 301  
 defined ..... 6-7, 233  
 direct collection ..... 240, 248, 250  
 disclosure ..... 113-136, 264-290, 326, 345  
     archival purposes ..... 282, 300-303  
     audits ..... 279-280  
     authority ..... 272-273  
     collecting fines or debts ..... 277-278  
     common programs and services ..... 276-277  
     compliance with enactments ..... 246, 270-272  
     compliance with subpoena, warrant  
         or order ..... 273-274  
     consent ..... 114-115, 269-270, 281  
     consistent use ..... 268  
     constraints on ..... 264, 276-277, 278, 300-302  
     correctional authorities or  
         institutions ..... 155, 156, 286, 288-289  
     court proceedings ..... 285-286  
     deceased individuals ..... 120, 290-292  
     delegation of authority ..... 27  
     Directory of Personal Information  
         Banks ..... 41-42, 234  
         discretionary benefits ..... 117, 118-120, 268  
         duty to assist ..... 50-51  
         emergencies ..... 115, 284  
         employee information ..... 115-117, 126,  
             141-143, 238  
         enforcing legal rights ..... 277  
         extent of ..... 294  
         expert consultations ..... 285  
         financial information ..... 125, 127  
         for investigations ..... 118-119, 282-284  
         forms ..... Appendix 5  
         for purposes of collection ..... 241-242, 268-269  
         guardians or trustees ..... 36  
     health or safety danger ..... 114, 115, 137-140  
         notices ..... 115  
     Internet ..... 265, 289  
     investigations ..... 350, 362-364  
     judicial tribunals ..... 285-286  
     labour unions ..... 272, 281  
     law enforcement ..... 282-284  
     legal matters ..... 277  
     legal proceedings ..... 277, 285-286  
     licences and permits ..... 118-119, 268  
     maintenance enforcement ..... 246-247, 287  
     making payments ..... 277-278  
     minors ..... 37-39  
     not contrary to public interest ..... 120-123, 278  
     not unreasonable invasion of  
         privacy ..... 113-136, 213-214, 267-268, 301  
     notices ..... 115, 218-219, 276, 345  
     Officers of the Legislature ..... 288  
     personnel management ..... 286-287  
     prior knowledge of information ..... 130  
     professional capacity ..... 128, 129  
     proof of identity ..... 35, 37, 38  
     protection of environment ..... 130-131  
     public events ..... 122  
     public health ..... 130-131  
     public information ..... 289-290  
     public interest ..... 120, 121, 267, 268  
         limitations ..... 227  
         limited disclosure ..... 227  
     public safety ..... 130-131, 137-140  
     public scrutiny ..... 130  
     quasi-judicial proceedings ..... 285-286  
     quasi-judicial tribunals ..... 285-286  
     reasonable expectations ..... 121  
     record of purposes ..... 303-304  
     records of ..... 266  
     refusal of consent ..... 270  
     request for non-disclosure ..... 123  
     research purposes ..... 284, 296-297, 326  
     restrictions on archives ..... 300-302  
     statistical purposes ..... 284, 296-297, 326  
     surveys ..... 334  
     third parties ..... 218-219  
     to avert imminent danger to health  
         or safety ..... 292  
     to bargaining agents ..... 281-282  
     to employees ..... 274-276, 354  
     to ministers ..... 274-276, 355  
     to MLAs ..... 280-281  
     to Ombudsman ..... 288  
     to Public Trustee ..... 246  
     to representatives ..... 36-39  
     unauthorized ..... 259, 266



- unreasonable invasion of privacy ..... 113-136, 151
  - criteria outside the Act..... 129-130, 129-130
  - determining..... 129-135
  - use after ..... 263
  - vehicle accidents..... 293
  - verifying eligibility..... 279
  - websites ..... 207
- discretionary benefits..... 117, 118-120
- disposition..... 259, 310-311
- errors..... 253-255
- health information ..... 7, 55-57
- honours ..... 122-123, 343
- identifying
  - for disclosure ..... 267-268
  - new uses ..... 260, 268-269
- inaccurate..... 134, 250-251
- inadvertent disclosure ..... 123
- in camera* meetings..... 173-175
- indirect collection ..... 234, 237, 240-248, 335
  - authorized by Information and Privacy Commissioner..... 234, 241, 350-351
  - authorized by enactments ..... 234, 241
  - authorized by individual..... 234, 241
- individually identifiable..... 297
  - removal of identifiers ..... 297, 298
- law enforcement records..... 124-125
- less than 25 years old..... 301
- licences ..... 118-119
- limitations on access..... 95
- linkage ..... 255, 297, 352
- minors..... 37-39
- notices to experts ..... Appendix 3
- offences ..... 44-45, 125, 235, 354, 362
- omissions..... 254
- opinions ..... 254-255
- permits ..... 118-119
- police officers..... 154
- power of attorney..... 37
- protection..... 324-325
  - electronic transmission ..... 40
  - physical security ..... 234, 259-260
  - records management system..... 312-313
- public interest
  - limited disclosure ..... 227
- records excluded from *FOIP Act*..... 234
- records more than 75 years old..... 301
- refusal to confirm or deny existence
  - of records ..... 135, 139
- refusal to disclose individual's own ..... 137-140, 141-144
- registries ..... 13-14
- request for non-disclosure ..... 123, 268
- research agreements
  - contents of ..... 299, Appendix 5
- retention..... 234, 252-253, 323-324
- routine disclosure..... 35, 267
- sharing by public bodies ..... 323, 329, 336, 325-330
- sole-proprietorship..... 113, 233
- supplied by applicant..... 134-135
- suppressing ..... 35
- taxes ..... 127
- third parties..... 32, 113, 218
  - consultations..... 211-224
- trustees..... 36, 246
- unauthorized access ..... 259
- unauthorized destruction ..... 259
- unreliable ..... 134
- updating..... 251-252
- use..... 259-264, 325-326, 345
  - consent to new uses ..... 261-263
  - constraints on..... 264, 294-295
  - correction..... 256
  - disclosed by other public
    - bodies ..... 263
    - fund-raising ..... 263-264
    - investigations..... 362-364
    - record of purposes ..... 323
    - unauthorized ..... 259
  - verification of ..... 251, 348
- verifying eligibility for programs or services..... 245-246, 279
- Personal Information Annotation**
  - Form** ..... Appendix 5
- personal information banks** ..... 25, 235, 261, 272
  - contents..... 272, 346
  - data matching..... 347
  - directories ..... 25, 41-42, 235, 303, 304, 309, 323, 347
  - local public bodies..... 41-42, 309
  - management..... 319
  - public bodies..... 41-42, 323
  - purposes..... 266, 303, 323
  - record inventories ..... 309
  - uses..... 261, 323
- Personal Information Protection Act (PIPA)** ..... 4, 235, 244
- Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)**..... 4, 244
- personal information requests** ..... 55-57, 268
  - correction..... 250-257
  - disregarding..... 59, 354
  - forms ..... Appendix 5
  - notices ..... Appendix 3
  - refusal..... 256

- transfers ..... 61-63, 259
- defined ..... 55
- fees ..... 74-75
- forms ..... Appendix 5
- refusal of access ..... 79, 88
- refusal to disclose applicant's
  - information ..... 137-140, 141-144
- representatives ..... 36-39, 55, Appendix 5
- responsive information ..... 84-85
- transfers
  - correction of information ..... 63, 259
- personal information sharing agreement** ..... 343
- personal information systems** ..... 319-348
  - contracting out ..... 333
  - reviews ..... 309-327
- personal notes** ..... 6
  - elected officials ..... 14
  - in camera* meetings ..... 175
- personal opinions, *see* **opinions**
- Personal Property Registry** ..... 13
- personal records, *see* **elected officials**, **personal records**, **governing bodies**, **personal records**; **ministers**, **personal records**
- personal service contracts** ..... 116, 118, 181, 247, 287, 289
- personnel information**
  - disclosure
    - not unreasonable invasion
      - of privacy ..... 115-117, 118, 267-268
    - unreasonable invasion of privacy ..... 126, 127
- personnel management**
  - administrative investigations ..... 254
  - audits ..... 195, 280
  - collection of personal information ..... 238-239, 247-248
  - disclosure of personal information ..... 286-287
  - grievances ..... 146
  - local public bodies ..... 287
  - plans ..... 181-182
  - security ..... 338, 339-340
  - third parties ..... 102
- personnel records**
  - employment history ..... 126
  - routine disclosure ..... 36
- persons with disabilities, *see* **disabled persons**
- photo radar** ..... 229
- photographs** ..... 6
  - class ..... 120
  - honours and awards ..... 123
  - promotional purposes ..... 270
  - students ..... 120
- physical health, *see* **health**
- physicians**
  - expert consultations ..... 138, 285
- PIPA, *see* **Personal Information Protection Act**
- PIPEDA, *see* **Personal Information Protection and Electronic Documents Act**
- plans**
  - budgetary ..... 177, 182
  - business plans ..... 167, 191
  - correctional facility ..... 154
  - information management ..... 307
  - Information Security Plan* ..... 336
  - negotiations ..... 177, 181
  - personnel management ..... 181-182
  - security systems ..... 155
  - technical ..... 104
- Police Act** ..... 4, 146, 153
- police and policing**
  - see also* **law enforcement**
  - criminal intelligence ..... 145, 151-152
  - defined ..... 145
  - delegation of FOIP responsibilities ..... 28, 29
  - informers ..... 150-151, 199-200
  - investigations ..... 145-147, 152, 237
    - completed ..... 158
  - peace officers ..... 153-154
  - police officers
    - personal information ..... 154
  - special constables ..... 141, 146, 154
  - video surveillance ..... 150, 237, 244
- police commissions** ..... 4, 130, 174
- police services** ..... 4, 282, 284
- policies and procedures**
  - advice and recommendations ..... 177, 178-180
  - archival records ..... 302
  - compliance with *FOIP Act* ..... 25
  - disclosure of course evaluations ..... 293-294
  - disclosure of information ..... 98
  - disclosure of personal information ..... 267-268
  - disclosure to MLAs ..... 280-281
  - information management ..... 308-314
  - information technology and systems ..... 308-309, 329
  - instructions or guidelines ..... 185
  - interpretation ..... 186
  - negotiations ..... 181
  - pending policy decisions ..... 182-183
  - personal information systems ..... 319-327
  - privacy protection ..... 331-333
  - records management ..... 305, 308-314
  - routine disclosure ..... 31-32
  - security ..... 259-260, 335-340
  - web sites ..... 334, 335
- policing committees** ..... 4

- policy advice**
  - background materials..... 179, 185
  - Executive Council or Treasury Board ..... 166-171
  - officials..... 177-187
- Policy for Maintaining Security of Government Data Stored on Electronic Data Storage Devices** ..... 255, 311
- Policy for the Transmission of Personal Information via Electronic Mail and Facsimile** ..... 217, 336
- political beliefs**..... 6, 128-129
- political parties**
  - membership ..... 128-129
- polls**
  - collection of personal information..... 236
- post-secondary educational bodies**
  - alumni records ..... 260, 263-264, 293
  - archives..... 300
  - calendars..... 249
  - class photographs..... 121
  - common programs or services..... 277
  - complaint process ..... 103
  - course books ..... 192
  - course evaluations ..... 293-294
  - economic interests ..... 192, 193
  - enrolment information ..... 121-122
  - fund-raising activities ..... 192
  - governing bodies ..... 15, 173
  - graduations
    - lists of graduates..... 121
  - heads..... 23-24
  - in camera* meetings, authority for..... 173-174
  - peer evaluations ..... 142
  - program eligibility ..... 141, 245
  - teaching and research materials ..... 11-12
  - teaching evaluations ..... 293-294
- Post-secondary Learning Act**..... 2-3, 173
  - section 65..... 236
- power of attorney**
  - exercising rights of individuals..... 37
- Powers of Attorney Act** ..... 37
- presumptions**
  - unreasonable invasion of privacy ..... 123-129
- pricing criteria**..... 107
- pricing structures**..... 103, 191
- prisons and penitentiaries, see correctional authorities or institutions**
- privacy**
  - audits ..... 251, 333, 351, 364
    - FOIP Coordinator ..... 25
  - compliance reviews ..... 319-327
  - deceased individuals ..... 120, 268, 290-292
  - harm..... 113-136
  - not unreasonable invasion of privacy ..... 113-123, 267
  - principles..... 233
  - protection..... 1, 25, 113-136, 233-304, 319-348
    - delegation of authority..... 27
    - information technology and systems ..... 155, 314, 319-348
    - monitoring ..... 351-352
    - notice in electronic form..... 40
    - offences ..... 44-45, 235, 353
    - policies and procedures ..... 332
    - public interest ..... 120-123, 225
    - reports to be published ..... 207-208
    - request for non-disclosure ..... 123, 268
    - technologies to enhance..... 327-328
    - unreasonable invasion ..... 113-136
      - criteria outside the Act ..... 129-130
      - determining..... 129-135, 151
- Privacy Act (Canada)** ..... 5
- privacy impact assessments**..... 237, 328-333, 340, 351
- Privacy Impact Assessment: Instructions and Annotated Questionnaire** ..... 331, 336
- privacy statements** ..... 334
- privatization** ..... 286
- privileged information**..... 196-205
  - case-by-case privilege ..... 200-201
  - common interest ..... 199
  - confidential informant privilege ..... 199-200
  - Crown privilege ..... 200
  - Information and Privacy Commissioner..... 353
  - law enforcement ..... 199-200
  - legislated privilege..... 201
  - litigation privilege ..... 198-199
  - parliamentary privilege..... 199-200
  - severing ..... 86, 204
  - solicitor-client privilege..... 197-198
    - lawyer's bill of account ..... 198
  - third parties..... 197-199, 202
    - private records ..... 200
  - waiver of..... 203
    - burden of proof..... 203
    - intention..... 203
- prizes**..... 242
- probate, see estates, administration of**
- probation** ..... 155, 156, 245, 289
- proceedings**..... 147
  - see also legal proceedings*
  - Proceedings Against the Crown Act,**
    - section 11 ..... 200
- products**
  - design..... 103
  - price regulation..... 107

- testing ..... 184, 191
- professions**
  - licences and permits..... 118, 268
- profit and loss statements**..... 103
- programs and services**
  - administration of personnel ..... 247-248
  - administrators ..... 25-26
  - applications for ..... 245
  - attendance ..... 122
  - collection of personal information..... 237-239
  - comments by Information and Privacy
    - Commissioner ..... 351-352
  - common programs ..... 276-277
  - continuing eligibility for ..... 245-246
  - eligibility..... 245-246, 251, 279, 295
  - evaluation ..... 269, 295
  - expansion ..... 295
  - FOIP contacts ..... 26, 234
  - integrated programs ..... 276-277
  - manuals and guidelines..... 42-43
  - plans..... 181
  - policies
    - interpretation ..... 186
    - rules ..... 186
- programs of study** ..... 126, 141
- property**
  - assessment information..... 295
  - in camera* meetings..... 174
  - licences and permits..... 118-119, 268
  - ownership ..... 269, 295
  - rental values..... 108
  - security ..... 121, 149, 155
- Proposal to Access Personal Information for Research or Statistical Purposes**
  - Form* ..... Appendix 5
- proprietary interest**..... 190-191
- proprietorships**
  - sole..... 113, 211, 233
- prosecution records**..... 12-13, 152-153
  - 10 years old or more ..... 153
- prosecutions**
  - appeal period ..... 12-13
  - decisions not to proceed ..... 158
  - discretion to proceed..... 152-153
  - protection from ..... 44
  - stays ..... 12-13
- Protection for Persons in Care Act**..... 147
- protection of personal privacy, *see* **privacy, protection**
- protests**..... 149
- Provincial Archives of Alberta**
  - church records ..... 12
  - disclosing business information..... 111
  - disclosing personal information to ..... 282
  - disclosure of personal information ..... 300-303
  - information 25 years old..... 301
  - labour union records..... 12
  - member of Executive Council records ..... 12
  - policies and procedures ..... 302
  - private records ..... 12
  - records 75 years old..... 301
  - records excluded from the Act..... 5, 12
  - transfer of records to..... 71, 282, 302, 310, 315, 316-317
  - unrestricted records ..... 301-303
- Provincial Court of Alberta**
  - excluded from *FOIP Act* ..... 4
  - FOIP offences..... 45-46
  - records ..... 9
- provincial governments**
  - intergovernmental relations ..... 161-164
- provincial health boards**..... 3
- Provincial Offences Procedures Act**..... 46
- provincial public bodies, *see* **public bodies**
- psychiatric information** ..... 124
- psychiatric institutions**
  - patients..... 154
- psychiatrists**
  - expert consultations ..... 138, 285
  - psychological information ..... 124
- psychological tests** ..... 195
- psychologists**
  - expert consultations ..... 138, 285
- public accountability, *see* **accountability**
- public bodies, *see also* local public bodies**
  - administration ..... 181-182
  - agreements
    - collection of personal information..... 235
  - annual reports ..... 207
  - assets..... 188, 190
  - business contact information ..... 290
  - business plans ..... 181-182, 191
  - competitive position ..... 191-192
  - commercial enterprises ..... 229
  - consultations or deliberations ..... 180-181, 214
  - decision-making processes ..... 177-180
  - defined ..... 2
  - Directory of ..... 30, 41-42, 323
  - discretionary benefits..... 117, 118-120
  - economic interests ..... 188-194
    - harms test..... 188-189
  - excluded from *FOIP Act* ..... 4-5
  - financial gain ..... 188
  - financial liabilities ..... 188
  - financial loss..... 188, 191-192
  - FOIP Coordinator ..... 24-25



- frivolous or vexatious requests ..... 58-59
  - harassment ..... 57-59
  - heads ..... 23-24
  - health information ..... 55-57
  - honours and awards ..... 122, 343
  - investment strategies ..... 189
  - internal activities ..... 247
  - liability ..... 95
  - manuals and guidelines accessing ..... 185
  - minutes ..... 177, 182
  - negotiations ..... 181, 191
  - non-arm's length transactions ..... 111
  - notices ..... Appendix 3
  - officers
    - disclosing personal information to ..... 274-276
  - personal information banks ... 41-42, 235, 272, 323
  - plans
    - implementation ..... 182
  - preparing for reviews ..... 357
  - programs and services, *see* **programs and services**
  - protection of privacy ..... 233-235
  - public scrutiny ..... 130
  - records management ..... 305-317
  - registries ..... 13-14
  - roles and responsibilities ..... 23-27
    - confidential information ..... 106
  - sharing of personal information ..... 329, 336
  - testing for purchase ..... 184, 193
  - trade secrets ..... 190
  - public college** ..... 3, 173
  - public events**
    - attendance or participation ..... 122
  - Public Guardian**
    - (Government of Alberta) ..... 246
  - public health**
    - disclosure of personal information ..... 130-131
    - fee waiver ..... 77, 79-81
    - inspections ..... 157
  - Public Inquiries Act** ..... 353, 359
  - public interest**
    - case-by-case privilege ..... 200-201
    - data linkage ..... 297-298
    - defined ..... 79
    - determination ..... 79-81, 229-230
    - disclosure ..... 225-232
      - mandatory exceptions ..... 96
    - notices ..... 39, 230-231
    - fee waiver ..... 79-81
    - not contrary to ..... 120-123, 268
    - personal information disclosure ..... 13, 120-123, 227, 267, 268
    - privilege ..... 200-201, 204
    - research benefits ..... 296
    - scope ..... 79
    - third party consultation ..... 230
  - public interest override** ..... 225-232
  - Public Lands Act** ..... 272
  - public meetings** ..... 173, 174
  - public order** ..... 145
  - public registries, *see* **registries**
  - public relations** ..... 26
  - public safety**
    - disclosure harmful to ..... 137-140
    - disclosure of personal information ..... 130
    - fee waiver ..... 77, 79-81
    - harm to ..... 225, 228
  - public scrutiny**
    - and privacy ..... 130
  - Public Trustee** ..... 246, 273
  - Public Trustee Act** ..... 246, 272, 273
    - section 44 ..... 246, 273
  - publications, *see* **reports and publications**
- Q**
- Qualicare Health Service Corp. v. Alberta (Office of the Information and Privacy Commissioner)** ..... 365
  - quality assurance committees** ..... 10
  - quality assurance records** ..... 10, 280
  - quasi-judicial tribunals** ..... 9
    - criteria for determining ..... 9-10
    - disclosure of personal information to ..... 285-286
    - draft decisions ..... 9
    - personal note ..... 9
    - rules ..... 5
  - Question Period** ..... 169
  - questions, from public** ..... 32
  - questionnaires**
    - collection of personal information ..... 236, 238
- R**
- R. v. Leipert** ..... 200
  - racial origin** ..... 128-129
    - personal information ..... 6
  - RCMP** ..... 5, 146, 202, 282, 284
  - real property, *see* **property**
  - recommendations**
    - Executive Council ..... 166-171
    - officials ..... 177-180
  - records**
    - 5 years old
      - Cabinet decisions ..... 101, 169, 170
    - 10 years old
      - prosecutorial discretion ..... 153

- 15 years old
  - administrative and management,
    - public body ..... 182
  - advice from officials ..... 101, 183
  - audit by Chief Internal Auditor ..... 19, 101, 186
  - Executive Council or Treasury Board ..... 101, 168
  - intergovernmental relations ..... 101, 164
  - local public body confidences ..... 101, 175
- 50 years old
  - businesses ..... 111
- 75 years old
  - personal information ..... 301
- access ..... 47-94
  - accuracy ..... 322
- Alberta Treasury Branch ..... 17
- alienation ..... 310
- alumni ..... 263-264, 293
- annotation ..... 255, 256-257
- attachments ..... 16-17
- available without FOIP request ..... 32
- banking ..... 17
- businesses ..... 101-104
- classification systems ..... 308-309
- compelling production ..... 353-354
- confiscated ..... 153-154
- constituency ..... 14, 15
- consultants ..... 7
- contractors ..... 45, 69-70, 314
- copying ..... 53, 69-70
- correction ..... 255, 322-323
- correctional records ..... 155-156
- counselors ..... 8
- courts ..... 9-11
- creating and generating ..... 7, 35, 73, 83-84, 309
- creation for ease of severing ..... 87
- credit unions ..... 17-18
- Crown ..... 200
- custody or control ..... 7-8, 45, 52
- defined ..... 6
- destruction ..... 6, 71, 239, 309-312, 316-317
  - documentation ..... 90, 306, 317
  - offences ..... 45, 71, 94, 259, 316
  - unauthorized ..... 259
- directories of holdings ..... 309, 323
- disclosure to Public Trustee ..... 246
- disposition ..... 6, 8, 70-71, 309-312, 316-317, 324, 346
  - FOIP requests ..... 93
- elected officials ..... 14-15
- election campaign ..... 15
- electronic ..... 6, 83-84
- examination of ..... 49
- fees ..... 74
- Information and Privacy
  - Commissioner ..... 353-354, 359
  - excluded from *FOIP Act* ..... 9-20, 91
  - excluded from Part 1 ..... 18-19
  - Executive Council ..... 15-16, 166-171
  - failure to locate ..... 89-90
  - falsification
    - offences ..... 45
  - FOIP requests ..... 87, 91
  - identification ..... 52
  - judicial administration ..... 9
  - justices of the peace ..... 9
  - labour unions ..... 12
  - law enforcement ..... 89, 124-125, 145-147, 153, 155, 158
    - records of disclosure ..... 284-283
  - legibility ..... 53
  - libraries ..... 12
  - line-by-line review ..... 82
  - linkage ..... 255-257, 297-298, 329, 352
  - locating ..... 52
  - medical ..... 200
  - ministers ..... 12, 18-19
  - MLAs ..... 16-17
  - modifying for routine disclosure ..... 35
  - not information ..... 226
  - not subject to FOIP ..... 53
  - offences ..... 45, 71, 94, 235, 335
  - personal information accuracy and ..... 234, 251-252, 322
    - compliance reviews ..... 319-327
    - correction ..... 253-259
    - disclosure for archival purposes ..... 282
    - retention ..... 234, 250-251
    - unauthorized destruction ..... 259
  - public events and activities ..... 122
  - Public Trustee ..... 246
  - purposes
    - background facts ..... 169
  - refusal to confirm or deny
    - existence ..... 89, 135, 139, 158
    - harm to health or safety ..... 92, 139
    - harm to law enforcement ..... 92, 158
    - notices ..... Appendix 3
    - personal information ..... 92, 135
    - unreasonable invasion of privacy ..... 87, 135
  - responsive information ..... 84-85, 86
  - retention ..... 6, 70, 234, 323-324
    - by Information and Privacy
      - Commissioner ..... 353-354
      - FOIP requests ..... 94
      - personal information ..... 250-253, 282, 323-324, 348



- retrieval.....69-70, 308-309, 314-315
- review of holdings.....33-34, 71
- routine disclosure.....5, 31, 31-35, 317
- scheduling.....316-317, 323-324, 348
- searching.....50-51, 52, 69-70, 308-309, 312-313, 314-315, 360
- security.....27, 235, 324-325
  - compliance reviews.....324-325
- storage.....6, 253
  - searching.....69, 314-315
- storage facilities.....8
- third parties.....101-104
  - sending to, to avoid Act.....45
- transfer.....6
- transfer to archives.....12, 302, 310, 315
- transitory.....239, 311-312, 316
  - local public bodies.....312
- Treasury Board.....166
- Records Alienation Schedule**.....310
- Records and Information Management Branch**,  
*see also records management*
  - publications.....94, 306, 308, 310, 312, 313, 336
- records management**.....26-27, 305-317
  - contracts and contractors.....314
  - Information and Privacy Commissioner.....306
  - information dissemination.....34
  - information technology and systems.....313-314
  - local public bodies.....6, 306
  - personal information banks.....309
  - policy and procedures.....26-27, 308-314
  - principles.....306-307
  - security.....312
  - systems.....308-309
- Records Management Regulation** ... 252, 253, 305, 306, 307, 310, 312
- recycling**.....311
- reference checks**.....142, 247, 252
- references**
  - character.....127-128
  - employment.....127-128, 141, 142, 242, 247, 252, 270, 286
- Refusal to Confirm or Deny Existence of Record (Model Letter J)**.....89, Appendix 3
- regional authority**.....3, 121
- regional health authorities**.....3, 56
  - disclosing personal information to.....272
  - privacy impact assessments.....329-330
- Regional Health Authorities Act**.....3
- regional services commissions**.....4
- register of electors**.....288
- Registrar**
  - Companies.....13
  - Corporations.....13
- Motor Vehicle Services.....13-14
  - office, defined.....14
- registrar, defined.....13
- Vital Statistics (district registrar).....13-14
- registries**.....13-14
  - companies.....13
  - corporations.....13
  - motor vehicles.....12, 13
  - defined.....13
  - land titles.....12
  - office, defined.....14
  - operated by a public body.....13
  - personal property.....13
  - records.....13-14
  - vital statistics.....13
- regulations**
  - drafts.....166, 172, 182
  - Executive Council.....166, 182
  - interpretation.....185
  - information readily available to public.....207
- relatives**.....246, 284, 290-291, 357
- relevant circumstances**
  - unreasonable invasion of privacy.....129-135
- religious beliefs**.....6, 128-129
- remote areas**
  - FOIP requests.....50
- repetitious FOIP requests**.....57-58
  - multiple applicants.....58
- reports and publications**
  - Alberta Health and Wellness, *see Alberta Health and Wellness*, publications
  - arbitration.....108-109
  - available for purchase.....207
  - completed research.....183
  - disclosure.....207
  - failure to publish.....209
  - fund-raising.....243
  - Information Management Branch, *see Records and Information Management Branch*, publications
  - inspections.....104
  - labour relations.....109
  - law enforcement.....157-158
  - Office of Corporate Chief Information Officer, *see Corporate Chief Information Officer*, policies
  - Office of Information and Privacy Commissioner, *see Information and Privacy Commissioner*, *IPC FOIP Practice Notes*
  - routine disclosure.....33
  - to minister.....16
- representatives**
  - authorization of.....36-39, Appendix 5
  - consent to disclosure.....115

- exercise of individual rights ..... 36-39, 79
- notices ..... 40
- personal information requests ..... 55, 89
- requesting reviews ..... 357
- reputation**
  - corporate or financial ..... 108
  - deceased individuals ..... 132
  - personal ..... 129, 134, 297, 298
  - public bodies ..... 192, 193, 314
- Request for Proposals** ..... 110
- Request Statistics Report** ..... Appendix 5
- Request Summary Form** ..... Appendix 5
- Request to Access Information Form** ..... Appendix 5
- Request to Correct Personal Information Form** ..... 255, 257, 258, Appendix 5
- research**
  - aboriginal claims ..... 129, 132
  - agreements ..... 298-299, Appendix 5
    - security ..... 298-299
  - background ..... 185
  - benefits to be in public interest ..... 298
  - business information ..... 111
  - genealogical ..... 120
  - grants ..... 119-120
  - historical ..... 120, 193
  - incomplete ..... 183
  - Information and Privacy Commissioner... 350, 352
  - medical ..... 193
  - methodology ..... 185
  - not unreasonable invasion of privacy ..... 300-301
  - personal information ..... 284
    - agreements ..... 298-299, Appendix 5
    - disclosure for ..... 297
  - priority of publication ..... 11, 193
  - public body employees ..... 192
  - purposes
    - personal information ..... 297
  - reports and publications ..... 183, 193
  - scientific ..... 185
  - teaching and research materials ..... 11
  - technical ..... 185
- resolutions**
  - drafts ..... 172-173
- response times** ..... 67
- Responses to Access Requests (Model Letters)**
  - Granting Access (Model Letter G)* ..... 89, Appendix 3
  - Access to All or Part of Record(s) Refused (Model Letter H)* ..... 20, 89, Appendix 3
  - Record does not Exist (Model Letter I)* ..... 88, Appendix 3
- responsive information, *see* **FOIP requests**, responsive information
- retention, *see* **personal information**, retention; **records**, retention
- retrieval of records, *see* **records**, retrieval
- revenue**
  - FOIP ..... 77
  - general revenue fund ..... 77
  - generation ..... 189
  - loss ..... 108, 191-192
- Revenue Canada *see* **Canada Revenue Agency**
- reviews** ..... 2, 30, 355-362
  - abandoning requests ..... 81
  - adequacy of search ..... 70, 315-316, 360
  - adjudication ..... 65, 365-366
  - correction of personal information ..... 255
  - disclosure of third party information ..... 221-222, 357, 358
  - documentation required ..... 358
  - evidence ..... 60, 316-317
    - in camera ..... 359
  - failure to disclose in public interest ..... 231, 351
  - fee estimates ..... 75-76
  - fee waiver requests ..... 77-81
  - notice ..... 39, 356, 357
  - preparing for ..... 357
  - privacy of deceased individuals ..... 356
  - process ..... 357-358
  - refusal ..... 359-360
  - refusing access ..... 96
  - requesting ..... 88, 356-357
    - forms ..... 365, Appendix 5
    - frivolous or vexatious ..... 360
    - time extension ..... 357
  - retention of records reviewed ..... 253
  - standing ..... 356
  - third parties ..... 65, 215, 216, 221, 355
    - decision to disclose information ..... 221-222
  - time extensions ..... 64-66, 216-217, 350, 356
  - time limits ..... 215-216, 357, 360
- right of access, *see* **access rights**
- routine access, *see* **routine disclosure**
- RFPs, *see* **Request for Proposals**
- routine disclosure** ..... 5, 25, 31-32
  - advantages ..... 31
  - creating new records ..... 35
  - delegation of authority ..... 34-35
  - historical practices ..... 98
  - information technology and systems ..... 313-314
  - inspections ..... 33
  - personal information ..... 35, 267
  - records management ..... 317
- Royal Canadian Mounted Police, *see* **RCMP**
- royalties** ..... 110
- rules of court** ..... 5

## S

- sabbaticals, *see* **employment**, educational leave
- sabotage** ..... 149, 152
- safety**
- disclosure endangering ..... 121
  - disclosure harmful to ..... 137-140, 268
  - harm to ..... 225, 228
  - imminent danger to ..... 292
  - inspections ..... 157
- Safety Codes Act**
- inspections ..... 157
- salaries and benefits** ..... 115-117, 126
- increments ..... 117
  - plans ..... 181-182
  - ranges ..... 115, 116-117, 126, 267
  - third parties ..... 103
- sanctions, *see* **penalties or sanctions**
- scholarships** ..... 119, 122, 141, 242
- Schedule 1 public bodies** ..... 25, 177, 182, 305, 307, 308, 309, 311, 313, 315
- Shields v. Information and Privacy Commissioner** ..... 365
- School Act** ..... 3, 38, 121, 184, 236
- school boards** ..... 3, 121
- appeals
  - reasons for decision ..... 184
  - employees ..... 103
- school trustees** ..... 14
- schools** ..... 126
- class photographs ..... 120, 249
  - closure ..... 68
  - council members ..... 103, 275
  - disclosing personal information, death of student ..... 265
  - enrolment information ..... 115-116
  - enrolment information ..... 121-122
  - graduations
  - lists of graduates ..... 120
  - registration ..... 261, 293
  - reunions ..... 121
- scientific information** ..... 103, 190-191
- Secretary to Cabinet**
- correspondence ..... 168
- Securities Act** ..... 21
- security**
- breaches ..... 338
  - Canadian ..... 149
  - communications systems ..... 159, 338-339
  - computers ..... 155
  - contracts and contractors ..... 339-340
  - defined ..... 155
  - electronic data ..... 26-27
  - harm to ..... 155
  - heads of state meetings ..... 149
  - information technology and systems ..... 259-260, 335-340
  - investigations ..... 145, 146, 155, 339
  - law enforcement ..... 145, 146, 155
  - local public bodies ..... 146
  - national ..... 149
  - penalties and sanctions for breach ..... 339-340
  - personal information ..... 234, 259-260, 324-325
  - compliance reviews ..... 324-325
  - research agreements ..... 298
  - physical ..... 259-60, 338
  - policies and procedures ..... 259-260, 335-340
  - property ..... 121, 155
  - in camera meetings ..... 174
  - records management ..... 26-27, 312
  - sporting events ..... 149
  - vehicles ..... 155
- Security of Information Act (Canada)** ..... 157
- Security Plan** ..... 336
- Security Policy For Disk Wiping Surplus Computers** ..... 311
- senior citizens**
- personal information ..... 272
- senior officers**
- disclosure statements ..... 11
- senior officials**
- advice and deliberations ..... 11, 177-187
- Seniors' Advisory Council of Alberta** ..... 16
- sensitive information**
- applicant identification ..... 89
  - exceptions to right of access ..... 32, 95, 98, 107, 124, 135, 162, 195
  - personal information ..... 124, 135, 337
  - proof of identity ..... 89
  - security ..... 259-260, 337
- service, *see* **notice**, service of
- Service Alberta** ..... 25, 60, 63, 163, 223, 287, 288, 295, 316, 366
- see also* **Access and Privacy; Records and Information Management Branch**
- severing information** ..... 85-87, 98
- FOIP Coordinator ..... 25
  - indicating ..... 53, 87-88
  - Information and Privacy Commissioner.. 357, 358
  - law enforcement records ..... 87
  - line-by-line review ..... 82-83, 100
  - manuals and guidelines ..... 43
  - non-responsive information ..... 85
  - privileged records ..... 204
  - procedures ..... 84, 85-86, 87
  - refusal of access ..... 86
  - solicitor-client privilege ..... 198

**sex**  
     personal information..... 6, 261  
**sheriffs**..... 153  
**shredding**, *see records*, destruction  
**smart cards**..... 352  
**smuggling**..... 151  
**social service benefits**..... 120, 125, 272  
     continuing eligibility for..... 245-246  
**software**..... 6  
     consideration of new..... 335  
     economic interests of public bodies..... 190  
     to verify accuracy of personal information 251-252  
**soil tests**..... 184, 193  
**solicitor-client privilege** ..... 197-198  
**Solicitor General**, *see Alberta Solicitor General*  
     and Public Security  
**spam** ..... 312  
**Speaker of the Legislative Assembly** ..... 4, 16, 350  
     office..... 16  
     parliamentary privilege..... 199-200  
     records excluded from *FOIP Act*..... 4, 16  
**special areas**..... 3  
*Special Areas Act* ..... 3  
**special constables** ..... 141, 146, 154  
**sporting events**  
     security ..... 149  
**spouse**..... 284, 293, 357  
**statistical information**  
     law enforcement ..... 158  
     personal information..... 284, 296  
     proprietary interest..... 191  
     surveys..... 185  
**statutory holidays**..... 68  
**storage**, *see records*, storage  
**stress**, *see health*  
*Stubicar v. Alberta (Office of the Information and Privacy Commissioner)*..... 365  
**Students Finance Board** ..... 263  
**Student Record Regulation** ..... 236, 241  
**student records**..... 275  
**students**  
     course evaluations ..... 293-294  
     death of..... 265  
     disclosure not unreasonable invasion  
         of privacy ..... 115, 116  
     emergency contacts..... 242  
     enrolment of..... 121-122  
     identification numbers ..... 261, 268  
     timetables..... 122  
**Subdivision and Development Appeal Boards** ..... 10  
**subpoenas**  
     disclosing personal information..... 273-274

**subsidiary health corporations** ..... 3  
**substance of deliberations** ..... 167-168  
     Cabinet confidences..... 166-171  
     local public body confidences ..... 172-176  
**suicide** ..... 137, 292  
**Superintendent of Financial Institutions (Canada)** ..... 282  
     supplied in confidence, *see confidential information*  
**Surplus Sales** ..... 311  
**surveillance**, video, *see video surveillance*  
**surveys**  
     collection of personal information..... 236, 238, 249  
     statistical..... 185  
     symbols, *see numbers or symbols*  
**systematic FOIP requests**..... 57-58

## T

**tax information**  
     disclosure ..... 109-110  
     personal information..... 127  
     rulings  
         routine disclosure ..... 33  
**taxes**  
     certificate ..... 109  
     collecting ..... 109-110, 189  
     determining liability ..... 109  
     returns..... 109  
**taxi licences**..... 118, 236  
**teachers**  
     certificates and permits..... 118  
     complaints ..... 128, 175  
     course development..... 191  
**teaching materials** ..... 11  
**technical information**..... 104, 191  
**technical institutes** ..... 3, 173  
**telecommunications**, *see communications systems*  
**telephone**  
     collection of personal information by..... 249  
**telephone directories**..... 289  
**telephone numbers**  
     personal information..... 6  
**temporary absence permits**..... 155  
**territorial governments**  
     intergovernmental relations ..... 161, 162  
**terrorism**..... 149  
**test banks** ..... 11  
**test results**..... 121, 184, 193, 195  
**testing procedures**..... 104, 195  
**tests**  
     environmental..... 184, 193, 195  
     fee for service ..... 184, 193  
     intelligence ..... 11, 195



- landfills ..... 184
- methods and procedures ..... 184, 193, 195
- products ..... 184, 193
- psychological ..... 195
- questions ..... 11, 195
- third parties**
  - burden of proof ..... 360-361
  - competitive position ..... 106-107
  - confidential information ..... 104-106, 132-133, 296
  - consent to disclosure ..... 110, 114, 220
  - consultations ..... 65, 211-224
    - non-response ..... 220
    - public interest ..... 230-231
    - responses ..... 219-220
  - custody of records ..... 6
  - disclosure of information authorized by
    - enactments ..... 111, 115
  - disclosure of information not unreasonable
    - invasion of privacy of ..... 113-123, 361
  - employees ..... 115, 116, 211
  - evaluations by ..... 127
  - financial gain ..... 108
  - financial loss ..... 108
  - harm to business interests ..... 96, 101-112, 212
  - identities ..... 217, 219
  - information jointly compiled ..... 104
  - labour relations ..... 108-109
  - multiple ..... 215
  - negotiating positions ..... 107, 191-192
  - notices ..... 40, 67, 211-224
    - content ..... 218-219
    - personal information ..... 115
    - public interest ..... 230-231
    - reviews ..... 355, 357
    - waiver of privilege ..... 203
  - personal information ..... 32, 113-136
    - correction ..... 257-258
  - personnel management ..... 103
  - privacy ..... 113-136
    - not unreasonable invasion ..... 113-123, 361
    - unreasonable invasion ..... 96, 123-136
  - privileged information ..... 197-199, 202
    - private records ..... 200
  - public events ..... 122
  - refusal to supply information ..... 107
  - research ..... 296
  - responses ..... 219-220
  - reviews ..... 355-358
  - routine disclosure ..... 32
  - tax information ..... 96, 109-110
  - time extensions ..... 65, 215, 216-217
  - time limits ..... 215-217
  - trade secrets ..... 102
  - threat and risk assessments ..... 337, 340-342
  - threats to security** ..... 147, 149
  - time extensions** ..... 64-67, 350
    - complaints ..... 59, 67
    - documenting ..... 67
    - investigations ..... 350, 362
    - limits on ..... 66-67
    - notices ..... 67
    - third parties ..... 65, 215, 216-217
  - time limits**
    - adjudication and adjudicators ..... 366
    - calculation ..... 216
    - complaints ..... 59, 364
    - compliance with Information and
      - Privacy Commissioner's Orders ..... 362
    - correction of personal information ..... 255, 257, 258
    - disregarding requests ..... 59
    - FOIP requests ..... 64-68, 72, 100, Appendix 4
    - judicial review ..... 364
    - producing records for the Information
      - and Privacy Commissioner ..... 353
    - requesting reviews ..... 357
    - reviews ..... 360
    - third parties ..... 215-217
    - transfers ..... 62
  - tracking systems, *see* **FOIP requests**, tracking
  - trade**
    - associated states ..... 149
    - deals ..... 189
  - trade secrets**
    - ownership ..... 101, 102, 190
    - public bodies ..... 190
    - third parties ..... 101-102
  - Traffic Safety Act** ..... 146, 147, 157
  - training** ..... 24, 30
    - personal information ..... 126
    - routine disclosure ..... 34
  - Transfer of Request (Model Letter C)** ..... 63, Appendix 3
  - transfers**
    - FOIP requests ..... 61-63, 71, 72
    - notices ..... Appendix 3
    - personal information requests ..... 61-62
    - correction of information ..... 259
  - Transitory Records Retention and Disposition Schedule** ..... 309
  - transitory records** ..... 252, 259, 311-312, 316
    - disposition ..... 70, 239, 311-312
  - Transitory Records Schedule** ..... 310, 312
  - Transmittal Memorandum (Sample)** ..... Appendix 5
  - Transportation, *see* **Alberta Transportation**
  - travel claims**
    - routine disclosure ..... 33

<b>Treasury Board</b>	
agenda.....	167, 168
background facts.....	168, 169-170
confidences.....	96, 166-171
decisions.....	167, 169-170
minutes.....	168
non-arm's length transactions.....	17
treasury branches, <i>see</i> <b>Alberta Treasury Branch</b>	
<b>treaties</b> .....	149
aboriginal people.....	162
disclosing personal information.....	270-271
law enforcement.....	284
<b>tribunals</b> .....	153
<b>trustees</b> .....	134
authorized representatives.....	36
exercising rights of individuals.....	36
<b>U</b>	
unemployment insurance, <i>see</i> <b>employment insurance</b>	
<b>UNESCO</b> .....	162
<b>United Nations</b> .....	162
<b>United States Immigration and Naturalization Service</b> .....	284
<b>United Way</b> .....	247
universities, <i>see also</i> <b>post-secondary educational bodies</b>	
educational bodies.....	2, 126
enrolment.....	121-122
reunions.....	121
<i>University of Alberta v. Pylypiuk</i> .....	130, 365
<b>unlawful acts</b> .....	154
<b>unsolicited information</b> .....	239-240
use of personal information, <i>see</i> <b>personal information, use</b>	
<b>V</b>	
<b>vehicles</b>	
accidents.....	293
security.....	148
vexatious FOIP requests, <i>see</i> <b>frivolous or vexatious FOIP requests</b>	
<b>video surveillance</b> .....	236, 237, 244
<b>video tapes</b> .....	259
<b>visually impaired persons</b>	
access.....	33
FOIP requests.....	49
<i>Vital Statistics Act</i> .....	12
<b>voice mail</b> .....	312

<b>volunteers</b>	
disclosure not unreasonable invasion of privacy.....	116
disclosure of personal information to.....	275
<b>vouchers</b> .....	6

## W

waivers, <i>see</i> <b>fees, waivers</b>	
<b>wardens</b> .....	153
<b>warrants</b>	
disclosing personal information.....	273-274
<i>Water Act</i> .....	147
<b>weapons</b>	
technical information.....	154-155
websites, <i>see</i> <b>Internet</b>	
welfare, <i>see</i> <b>social service benefits</b>	
<b>whistle-blowing</b> .....	43-44, 352-353
<b>Wigmore's test</b> .....	200-201
<b>wiretaps</b> .....	150, 157
<b>witnesses</b>	
compelling attendance.....	353, 359
protection.....	137
statements.....	237
<i>Workers' Compensation Act</i> .....	238, 241, 273
<b>workers' compensation claim</b> .....	277
<b>work experience programs</b>	
personal information.....	116, 277
written authorization, <i>see</i> <b>authorized representatives, written</b>	

## X

<b>x-rays</b> .....	6
---------------------	---

## Y

<i>Youth Criminal Justice Act (Canada)</i> .....	157, 354
<i>Youth Justice Act</i> .....	154









Printed on Recycled Paper 